**Indian Overseas Bank**
**Digital Banking Department**
**Central Office, Chennai**

# Policy on Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transaction

## 1. Introduction

With increasing thrust on promotion of digital banking transactions and customer protection, there has been an upward surge in the number of customer grievances relating to unauthorised transactions, resulting in debit of their accounts maintained with the bank, due to transactions not initiated by them through different kinds of electronic modes viz., cards, e-com, POS, Payment systems etc. This has necessitated the review of various aspects of customer protection and criteria for determining the customer liability in such unauthorised electronic banking transactions reported by the customers and to frame a Corporate Policy in limiting the liability of the customers in such transactions.

This Policy is framed on the regulatory requirements as enunciated by Reserve Bank of India (RBI) vide their circular bearing reference: DBR.No.Leg.BC.78/09.07.005/2017-18 dated 6th July 2017. This policy covers aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities, and customer liability arising in specific scenarios of unauthorized electronic transactions.

## 2. Types of electronic banking transactions:

Electronic banking transactions can be broadly classified into two categories:

(i) 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.) and

(ii) 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).

## 3. System and procedures for Safe Electronic banking:

Electronic banking transactions are happening in a secure mode with valid credentials like Card No., CVV, PIN, OTP.

**Robust and dynamic fraud detection and prevention mechanism is in place in the form of tools like Visa Risk Management – Visa, Enterprise Fraud Risk Management – NPCI, The Fraud Centre – Mastercard. Bank has procured additional Enterprise Fraud Risk Management Tool to monitor transactions made from cards as well as**

**other digital channels. Monitoring on real time basis is in place and various rules are implemented in these tools to prevent frauds.**

Appropriate measures to mitigate the risks and protect the customers against the liabilities arising therefrom is ensured by various awareness programs implemented and bank keeps creating awareness among the customers regarding frauds by displaying the notices, sending SMS, publishing in websites etc.

Apart from the above a Bankers Indemnity Insurance Policy coverage is taken by Banking Operations Department which includes the claims related to Unauthorized electronic banking transactions. Insurance Claims are to be preferred by Digital Banking Department and monitored by Banking Operations Department.

**4. Reporting of unauthorised transactions by customers to Bank**

The Bank is committed to ensure safety and security of electronic banking transactions carried out by its customers; and shall act upon the unauthorised electronic banking transactions reported by the customers to the bank, based on the time of reporting, evidences and supporting documents submitted along with the complaints.

As per the RBI guidelines any transaction claimed as unauthorized debit, customer has to report to bank within 30 days to be eligible for compensation. The transactions which are not intimated to bank will be deemed as undisputed.

Genuine and fraudulent transactions are differentiated on the basis of analysis of the pattern of transactions on the basis of amount, velocity/frequency, geographical feasibility of the transaction. A Standard Operating Procedure (SOP) is in place on "Handling claims on account of Unauthorised Electronic Banking Transactions" where the procedures to differentiate the genuine and fraudulent transactions.

**4.1 Registration of Customer Mobile Number and Sending SMS Alert by Bank:**

The Bank will ask the customers to mandatorily register for SMS alerts, while the email alerts will be sent wherever registered by the customers. The bank will not provide fresh digital facility of ATM Debit / Credit Card to customers who do not provide mobile numbers to the bank. Branch to obtain a suitable letter from the customer who is not willing to provide the mobile number and attach the same with account opening form.

In the cases where customer reports unauthorized transactions in his/her account but SMS not received due to non-registration of mobile number by the branch concerned, despite customer having provided mobile number, then the branch is liable for such omissions.

इण्डियन ओवरसीज बैंक
Indian Overseas Bank
12 MAY 2023
BOARD MEETING
मंडल की बैठक

**4.2 Notification of unauthorised electronic transactions by customer to Bank:**

The Bank requires customers to notify the Bank about any unauthorised electronic banking transaction, immediately after the occurrence of such transaction, as longer the time taken to notify the bank, the higher will be the risk of loss to the bank/customer.

To enable this to be done in a smooth and efficient manner, the Bank will provide customers with 24x7 access through multiple channels (via Bank's official website, e-mail, a dedicated toll-free helpline, reporting to home branch in person during the working hours etc.,) for reporting unauthorized transactions that have taken place and/or loss or theft of payment instrument such as card, etc.

Additionally, customer will be provided with various options/channels to block his Debit/Credit card, when he suspects some unauthorized transactions. Presently such blocking facility is available to branches and also provided in Bank's website, through Phone Banking facility (IVRS), in Internet banking facility, in mobile banking facility, Toll free number, etc.

Further, the Bank will provide a direct link for lodging the complaints, with specific option to report unauthorized electronic transactions in the home page of the Bank's website.

Immediate response (including auto response) will be sent to the customers acknowledging the complaint along with the registered complaint number.

On receipt of report of an unauthorized transaction from the customer, the Bank will take immediate steps to prevent further unauthorized transactions in the account/card by blocking the card or relevant channels.

Regional Offices concerned have to keep record of all cases reported and the status of FIR filed by the customer. A circular issued by the department in this regard has to be scrupulously followed.

As the CCTV footages are playing vital role in deciding the incident is fraud or not, branches have to keep the working status of the CCTVs in good condition. Branches and Regional offices to be held liable for any non-submission of the required footages.

Branches to clearly guide the customers on the risk involved in sharing the credentials which lead to fraudulent transactions by card cloning and data theft. However, the burden of proving the customer liability in case of unauthorized electronic transaction shall lie with the bank.


**5. Liability of a Customer of Bank in unauthorized electronic Banking Transaction**

**a) Zero Liability of a Customer**

A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:

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

ii. 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.

** (A glossary to important terminologies are provided as Annex -1)

**b) Limited Liability of a Customer**

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

i. In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, clicked on a Link sent by strangers, and/or entered payment credentials, and/or installed screen sharing application, etc., the customer will bear the entire loss until he reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.

ii. 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 Table 1, whichever is lower.

**Table 1 - Maximum Liability of a Customer under paragraph 5(b)(ii)**

| Type of Account | Maximum liability (₹) |
|---|---|
| • BSBD Accounts | 5,000 |
| • All other SB accounts<br>• Pre-paid Payment Instruments and Gift Cards<br>• Current/ Cash Credit/ Overdraft Accounts of MSMEs<br>• 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<br>• Credit cards with limit up to Rs.5 lakh | 10,000 |

| | |
|---|---|
| • All other Current/ Cash Credit/ Overdraft Accounts<br>• Credit cards with limit above Rs.5 lakh | 25,000 |

iii. Further, if the delay in reporting is beyond seventh working day, the customer liability shall be determined as under:

The customer will bear the entire loss until he reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank. However, depending on case to case basis, Bank may compensate customer an amount of maximum Rs 10000/- (Rupees Ten Thousand only) (if reported within 30 days) irrespective of the fact whether there is single or multiple number of transactions or transaction amount whichever is lower and the customer shall be entitled for such compensation only once in the customer's life time.

**c) Overall liability of the customer in third party breaches**, as detailed in paragraph 5(a) (ii) and paragraph 5(b) (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:

**Table 2 - Summary of Customer's Liability**

| Time taken to report the fraudulent transaction from the date of receiving the communication | Customer's liability (₹) |
|---|---|
| Within 3 working days | 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 and within 30 days | Unlimited.<br>(Bank may compensate a sum not exceeding Rs.10,000/-<br>,Rupees Ten thousand only) |

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.

**To determine the extent of a customer's liability, the communication systems used by the bank to send alerts and receive their responses thereto must record the time and date of delivery of the message and receipt of customer's response, if any, to them.**

**6. Reversal Timeline for Zero Liability/Limited Liability of customer**

On being notified by 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). **Digital Banking Department shall permit such shadow credit for all digital channels except AEPS, for which, Financial Inclusion Department will permit such shadow credit. DBD will maintain SOP on Accounting procedures.**

Bank may also at its discretion decide to waive off any customer liability in case of unauthorised 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.

**7.** Further, the bank shall ensure that:

i. a complaint is resolved and liability of the customer, if any, established within a period of 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraphs 5 and 6 above.
ii. where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 5 and 6 above is paid to the customer; and
iii. 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.
iv. a customer shall be eligible for compensation from the bank only once during the period of his/her banking relationship with the Bank.

For all disputed cases, customer shall be required to lodge a written complaint in his/her home branch or send email to bank from email address registered with the bank, along with supporting documents namely dispute form, copy of the police complaint duly acknowledged by the Police Department (copy of FIR or online Cybercrime complaint mandatory for claims of Rs. 50,000/- and above. For amount less than Rs. 50,000/-, complaint letter acknowledged by Police to be submitted) and other available evidence, within thirty calendar days, from the date of giving first intimation of the fraud by him/her to the Bank.

In case the customer is unable to provide the documents or there is a delay on part of the customer in submitting the documents within the afore said thirty days, the Bank shall term such disputes as unable to conclude and the liability of the unauthorized transactions in such cases will remain with the customer only.

इंडियन ओवरसीज बैंक Indian Overseas Bank
12 MAY 2023
BOARD MEETING
मंडल की बैठक

**7 (A): <u>International ECOM Transactions without 2FA:</u>**

In case of transactions occurred on the account of the customer by means of the unsecured Ecom transactions originated in the foreign websites without the Second Factor Authentication (2FA), and when a customer claims that an unauthrosied transaction, bank will shift the liability to the merchant as per the consortia guidelines. The cases, only in which the bank has the charge back rights with the consortia may entertain the customer for compensation on the amount claimed as unauthorized. In such situations bank will reimburse the customer to the extent of amount received in the charge back claim on a particular

transaction. Where the bank has no charge back rights will not entertain such claims.

**7 (B): Cash withdrawal from non-EMV compliant ATM Machine:**

In case cash withdrawal is made from non-EMV compliant ATM Machine, and the transaction is reported as unauthorized by the card holder, bank will shift the liability on the Acquirer Bank by raising charge back under EMV Liability Shift as per consortia guidelines.

**8. Discretionary Powers:**

As a measure of our Bank's commitment to speedy customer service, the customer will be compensated to the extent of amount as mentioned below where unauthorized electronic banking debits have taken place in the customer's account, after getting necessary approval from the appropriate layer of authority mentioned below,. to debit the "Customer Compensation Reimbursement for Electronic Banking Transactions A/C – CCR EBT A/c":

a. Regional Heads - up to Rs.50,000/-
(SRM Rs.25,000/- , CRM Rs.50,000/-)
b. General Manager, up to - Rs.1,00,000/-
c. Executive Director, up to - Rs.3,00,000/-
d. M D & CEO, up to - Rs.7,50,000/-
e. MCB - Above Rs.7,50,000/-

**The decision to write off the entries outstanding in the CCR EBT A/c identified as not recoverable may be taken, based on the amount required to be written off, in each individual case, by appropriate committee as per the extant guidelines issued by Banking Operations Department from time to time.**

Write off entries to be reported to ACE on monthly basis and quarterly report on write off accounts to submitted to ACB.

**9. Communication of the Policy:** The Bank shall provide the details of this policy in regard to customers' liability formulated in pursuance of RBI directions at the time of opening the accounts. Bank shall also display its approved policy in public domain through Bank's official website www.iob.in for wider dissemination and the existing customers shall also be individually informed about the bank's policy through SMS and/or e-mail wherever possible.

**10. Reporting and Monitoring Mechanism:** Customer liability cases shall be periodically submitted to the Customer Service Committee of the Board on a quarterly basis. 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.

Indian Overseas Bank
12 MAY 2023
BOARD MEETING
मंडल की बैठक

केन्द्रीय कार्यालय
CENTRAL OFFICE

The Standing Committee on Customer Service shall periodically review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redressal mechanism and take appropriate measures to improve the systems and procedures. All such transactions shall be reviewed by the bank's internal auditors/statutory auditor also. Internal auditors will review such cases settled under this policy during their regular audit of the bank and their report shall include details of any deviation from the directives stipulated in the policy.

**11. Linkage to other Customer Service Policies of the Bank:** This Policy shall be read in conjunction with the Customer Compensation policy and Customer Grievance Redressal policy issued by the Customer Service Department of the Bank.

**12. Validity of the Policy:** The policy shall be valid for a period of 36 months from the date of approval by the Board and shall be reviewed every year, with MD & CEO of the Bank having the discretion to extend it for further period of six months from the end date of its validity.

**********

इण्डियन ओवरसीज़ बैंक
Indian Overseas Bank
12 MAY 2023
BOARD MEETING
मंडल की बैठक

**Annexure – I**

**Glossary on important terminologies:**

| Terminology | Explanation |
|---|---|
| **Unauthorised Electronic Banking Transaction** | A financial or nonfinancial transaction taking place in the Bank account of a customer, through any type of electronic mode of payment, that was not done by the customer or his authorized agent or done without the customer's knowledge or authorization. |
| **Contributory Fraud** | Involvement of Bank staff in wrongful or original deception, intended to result in financial or personal gain |
| **Negligence** | Means one or combination of more than one of the following: lack of proper care and attention, dereliction of duty, non-performance or non fulfilment of duty, acts of laxity, irresponsibility, inattention, inattentiveness, thoughtless-ness, unmindfulness or forgetfulness. |
| **Deficiency** | Deficiency is any fault, imperfection, shortcoming or inadequacy in the quality, nature and manner of performance which is required to be maintained by or under any law for the time being in force or has been undertaken to be performed by a person in pursuance of a contract or otherwise in relation to any service – as per Sec 2(1) of the Consumer Protection Act 1986. |
| **Third Party Breach** | Third party breach means where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system. |
| **Service** | Service means service of any description which is made available to potential users and incudes facilities in connection with banking, financing but does not include the rendering of any service free of charge or under a contract of personal service – as per Sec 2(1) (o) of the Consumer Protection Act 1986. |
| **Payment Credentials** | Payment credentials are the confidential information like ATM PIN, CVV, OTP, UPI PIN etc., which are the unique, exclusive and secretive possessions of an individual customer, required for effecting a payment through electronic mode. |