

FAQ on Policy on Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transaction

1. What is an unauthorised transaction?

➤ Any transaction that is not authorized by the account holder can be termed as unauthorized transaction. An unauthorised transaction is the one, done by someone who somehow obtains the confidential data of the account holder and uses it to make transactions.

2. Does the bank have any policy for compensating its customer when unauthorized transaction on digital channels is reported by the customers?

➤ Yes. Our Bank has a Policy on Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions. The policy is available in our bank's website in the following location: www.iob.in → Customer's Corner → Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transaction

3. What types of unauthorised electronic transactions done through which channels are covered under this policy?


➤ Unauthorised Electronic Transactions done through the following channels are covered under the policy :

- i. Debit / Credit / Prepaid Card – Ecom / POS / ATM
- ii. Internet Banking
- iii. Mobile Banking
- iv. UPI (Unified Payment Interface)

4. What are the responsibilities of a customer with regards to his digital assets like credit card, debit card, internet banking username password, UPI PIN?

➤ Customer is expected to follow the following Safe Banking Practices :

- i. Keep the card details and card PIN Confidential
- ii. Never hand over the Debit / Credit to any third person or stranger
- iii. Not to write Card number, Card expiry date, Card CVV, UPI PIN, Fund Transfer PIN or any such details anywhere.
- iv. Never to reveal the UPI PIN to anyone.
- v. Not to enter the UPI PIN **for receiving funds**. UPI PIN is always used only for making Payments / Debit Transactions from your Account.
- vi. While attempting to reach customer care of any website/merchant, always take the number from the official website of the Bank. Contact Numbers available in Search Engines like "Google" can be incorrect and may direct the call to fraudsters.
- vii. Be aware of fake or fraudulent websites resembling the original website of the Bank.
- viii. Not to install screen sharing apps like Anydesk / TeamViewer etc. in the name of KYC verification. Such applications can be used to give remote access of your device to the caller, which may lead to collecting all your confidential information & data and result in unauthorized transactions.

- ix. Not to provide any sensitive information to strangers sending emails & asking for confidential information. They may be Phishing attempts to dupe you to collect your credentials for doing fraudulent digital transactions.
- x. To access the Bank's website only by typing the URL in the address bar of your browser.
- xi. To ensure that the URL on the address bar starts with 'https', and features a Green Padlock Icon 

5. What can a customer do if he/she has revealed card / UPI / Mobile Banking / Internet Banking credentials accidentally?

- In case a customer has been a victim of fraud, the Bank requires customers to notify the Bank about such 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.
- In such a case, the very first thing a customer must do is to block the access of the particular channel to stop further debits. Customer can block respective channels through following mediums:
 - i. Mobile Banking – Cards and Mobile Banking
 - ii. Internet Banking – Cards and Internet Banking
 - iii. BHIM IOB UPI – UPI Channel only
 - iv. 24X7 Toll Free Number – 044 – 28889314 – All Channels
 - v. Send an email to atmcard@iob.in from your registered email address to block your account – Cards
 - vi. Giving an application to any branch in person during working hours – All Channels
- After blocking the relevant channel, customer should report the unauthorized electronic banking transaction to the bank.

6. How can a customer report unauthorized electronic banking transaction?

- Unauthorized electronic banking transaction can be reported through any of the following mediums:
 - i. 24X7 Toll Free Number – 044 - 28889314
 - ii. Bank's Website – www.iob.in → Customer Complaints
 - iii. Send an email from registered email address to cybercell@iob.in or to the home branch
 - iv. Giving an application to any branch in person during working hours

7. In how many days does the customer have to report unauthorized transaction to the bank?

- Any transaction claimed as unauthorized debit has to be reported to bank within 3 days from the date of occurrence of the unauthorised transaction, to become eligible for 100% compensation claim.
- The unauthorised transactions which are not intimated to the Bank within the stipulated time lines, as mentioned in the following table will not qualify for claiming compensation.

- If such transactions are not reported within thirty days of occurrence, they will not be treated as disputed, if raised at a later date and no compensation is payable by the Bank. Entire liability will be that of the customer.

8. Can the customer report any time within these 30 days to seek full reversal of the amount or the reversal of the amount is based on some time criteria?

- The customer's liability will be calculated based on the date of giving first intimation of the fraud by him/her to the Bank. The overall liability is summarised in the below Table-1,

Table 1 - 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 <u>Table 2</u> , whichever is lower
Beyond 7 working days and within 30 days	Unlimited. (Bank may compensate a sum not exceeding Rs.10,000/-, Rupees Ten thousand only)

When there is a delay (of four to seven days after receiving 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 the below Table 2, whichever is lower.

Table 2 - Maximum Liability of a Customer under paragraph 5(b)(ii)	
Type of Account	Maximum liability (₹)
• BSBD Accounts	5,000
• 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	10,000

<ul style="list-style-type: none"> • All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh 	25,000
---	--------

9. Under what circumstances customer has to bear the responsibility of the loss incurred in the unauthorized transactions?

- The customer will bear the entire loss if he/she reports the incident after 30 days from the date on which the unauthorised transaction happened.

10. What documents does the customer have to submit to the bank / branch on which the bank can start processing the complaint of the customer?

- The customer has to submit the following documents to the bank:
 - i. Written complaint in home branch, or an email to home branch or cybercell@iob.in from registered email address of the accountholder.
 - ii. Copy of Police complaint filed by the customer (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 can be submitted)
 - iii. Any other evidence which may help investigate the case

11. Within how many days does the customer need to provide the documents to bank?

- The customer need to provide the documents within 30 calendar days from the date of giving first intimation of the fraud to the Bank

12. Is formal FIR mandatory in all the unauthorized transaction complaints?

- For amount less than Rs50000, Customer is required to submit Complaint letter acknowledged by Police, and for amount Rs50,000/- and above, copy of FIR or online Cybercrime complaint is mandatory.

13. Does the customer have to physically visit the Police Station to lodge police complaint or are there any other online channels for police complaint?

- The customer can visit <https://cybercrime.gov.in> OR can call at National Helpline Number – 155260 or 1930 which comes under Ministry of Home Affairs, Govt. of India. Alternatively, customer may also lodge online cybercrime complaint through state police website/email.

14. Within how many days can the customer expect the amount to be reversed to his account?

- Shadow credit is given within 10 working days from the date on which the customer notifies the branch and the actually credit is given to the customer within 90 days after arriving the eligibility of the customer as per the bank's compensation policy.

15. What is shadow credit?

- Shadow credit is the amount which the customer has reported lost which will be credited to customer's account with debit blocked for that amount.

16. In how many days does the bank have to complete the entire process of investigation and compensation?

- Bank has to complete the entire process of investigation and compensation to customer within 90 days.
- Bank shall arrive at the compensation amount based on its policy conditions and the eligible compensation amount will be unblocked and released to the customer.

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

/**\$**//