Customer Protection Policy (Unauthorized Electronic Banking Transactions)

Updated: June 2023

1. Introduction:

With the increased thrust on Digital Payments and considering the surge in customer grievances relating to unauthorized transactions resulting in debits to their accounts / cards / UPI/ mobile wallets, the criteria for determining the customer liability in these circumstances have been reviewed for electronic banking transactions.

Taking into account the risks arising out of unauthorized debits to customer accounts owing to customer negligence / Bank negligence / banking system frauds / third party breaches, the rights and obligations of customers in case of unauthorized transactions in specified scenarios, aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorized electronic banking transactions were reviewed and a policy was prepared in line with the RBI notification dated RBI/2017-18/15 BR.No.Leg.BC.78/09.07.005/2017-18 July 6, 2017 on Customer protection-Limiting Liability of customers in unauthorized Electronic Banking Transactions.

2. Objective of the Policy:

This policy document aims to provide framework on limiting liability of customers against the risks arising out of unauthorized debits to customer accounts owing to unauthorized electronic banking transactions due to customer negligence / Bank negligence / banking system frauds / third party breaches and to clearly define the rights and obligations of customers in case of unauthorized transactions in specified scenarios to use electronic banking channel.

It also defines the maximum customer liability for the electronic banking transactions to make customers feel safe about carrying out electronic banking transactions. This is intended to provide boon to customer service to make customers feel safe about carrying out electronic banking transactions which helps to increase the trust in Digital payments and deepen the digital payments of the Bank.

3. Scope/Coverage:

Electronic Banking Transactions generally covers transactions through following modes-

i) Remote/ Online Payment Transaction (e.g. Mobile Banking, Card not present Transactions, Internet Banking, Pre Paid Payment Instruments etc.)

ii) Face to Face/ Proximity Transaction (e.g. ATM, POS, QR code based Transactions etc.)

iii) Any other transaction done by electronic mode and accepted by the Bank for debiting/crediting customer account.

4. Right and Obligation of customer in case of unauthorized electronic banking transaction in specified scenario:

i) **Scenario 1: Customer Negligence –**

Unauthorized Electronic Banking Transaction happened due to customer negligence (such as where he has shared the payment credentials – card number, expiry period, OTP, clicked on unknown links etc.) Customer is required to be vigilant while doing electronic banking transaction and needs to ensure that the mobile number is registered with the bank and that checks the SMS alerts/statement of the accounts. Customer needs to immediately block the digital channel as per Table 3 of Annexure 1 and mandatorily register/ lodge the complaint under unauthorized transaction category with the Bank/ Branch/ Contact Center, etc. as per available channels mentioned in Table 4 of Annexure 1.

Customer Liability – 100% of the unauthorized electronic banking transaction amount will be customer liability and this will be notified to the customer as response to the customer complaint and the complaint will be treated as closed by the Bank.

Customer Right – Customer has to bear the entire loss of the transaction amount until he / she reports the unauthorized electronic banking transaction to the Bank/ Contact Center/ Branch, etc. where the negligence lies with the customer. Any loss (upto the value dated transaction amount) occurring after the reporting of the unauthorized electronic banking transaction to the Bank/ Contact Center/ Branch etc., shall be borne by the Bank; if the channel or product wherein the unauthorised electronic transaction has not been blocked or no action initiated by the bank branches/ contact center etc.

Customer Obligation – Customer to minimize his loss is required to approach the Bank/ Contact Center/ Branch, etc., as soon as the customer is aware about the unauthorized debit for blocking of the digital channel as per Table 3 of Annexure 1 and mandatorily register/ lodge the complaint under unauthorized transaction category with the Bank/ Branch/ Contact Center, etc as per available channels mentioned in Table 4 of Annexure 1.

ii) **Scenario 2: Bank's Negligence –**

Unauthorized Electronic Banking Transaction happened due to Contributory fraud / negligence / deficiency on the part of the Bank (either committed by Bank staff or Bank vendor) – (irrespective of whether or not the transaction is reported by the customer):

Customer Liability – Zero Liability

Customer Right – In such cases where customer has suffered loss due to Contributory fraud / negligence / deficiency of system on the part of Bank's system/ Branch/ Contact Center, etc. Customer is having right to get the compensation from the Bank as per referenced RBI circular which is limited upto the value date transaction amount of the unauthorised electronic banking transaction.

Customer Obligation – Customer is required to check the SMS / Email alert/ account statement and has to approach the Bank/ Contact Center/ Branch, etc. as soon as the customer aware about the unauthorized electronic banking debit transaction for blocking of the digital channel as per Table 3 of Annexure 1 and mandatorily register/ lodge the complaint under unauthorized transaction category with the Bank/ Branch/ Contact Center, etc. as per available channels mentioned in Table 4 of Annexure 1.

iii) **Scenario 3: Third Party Breach –**

Unauthorized Electronic Banking Transaction happened due to Third party breach where the deficiency lies neither with the Bank nor with the Customer but lies elsewhere in the System. Customer needs to immediately block the digital channel as per Table 3 of Annexure 1 and mandatorily register/ lodge the complaint under unauthorized transaction category with the Bank/ Branch/ Contact Center, etc. as per available channels mentioned in Table 4 of Annexure 1.

Customer Liability – Customer Liability will be ascertained based on the time taken by the customer to report the unauthorized electronic banking transaction as per Table 1 & Table 2 mentioned in Annexure 1.

Customer Right – In such cases where customer has suffered loss due to third party breach where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system, and the customer has notified the Bank **within seven working days**. Customer is having the right to get the compensation from Bank, which is limited upto the value date unauthorised electronic banking transaction amount as per Table 1 & Table 2 of Annexure 1. In such cases where customer has notified the unauthorized transaction to Bank after 7 days, Bank will have no liability, and this will suitably be communicated to the customer. Bank will try to pass the customer claim through Bank's Insurance Agency/ NPCI Chargeback process for that channel if available on best effort basis.

Customer Obligation – Customer is required to check the SMS / Email alert/ account statement and approach the Bank as soon as the customer becomes aware of the unauthorized electronic banking transaction debit for blocking of the digital channel as per Table 3 of Annexure 1 and mandatorily register/ lodge the complaint under unauthorized transaction category with the Bank/ Branch/ Contact Center, etc. as per available channels mentioned in Table 4 of Annexure 1.

5. Process for Shadow reversal of unauthorised electronic banking in customer's account:

i) If customer negligence been observed, then Bank will treat such cases as 100% customer liability and shadow credit in customer's account will not be given.

ii) If, it is limited liability case (scenario 2 and 3) then Bank is required to give shadow credit of amount limited to the unauthorised electronic banking transaction as applicable to customer account within 8 working days from the date of such notification by Customer. Respective Digital Group Channel team of Bank will reverse the amount from customer's account or realize the shadow credited amount in customer account within 85 working days basis the ascertaining of the evidences of the transaction.

6. Dispute Resolution Process- Notifying the Bank in respect of Unauthorized Electronic Banking transaction:

i) Customer is required to immediately report the unauthorized electronic banking transaction through various channels provided by the Bank and displayed at Bank website.

ii) On receipt customer's complaint (notification), Bank will take immediate steps to prevent further unauthorized transaction in the account and by blocking/ deregistering customer from notified electronic channel.

iii) The timeline for resolving all such complaint will be 90 days from the date of receipt of the complaint. Customer is required to provide following details to report the unauthorized transaction-

- ✓ Channel details like channel name, location etc.
- ✓ Transaction details like transaction type, account, date, amount etc.
- ✓ Fraud incident details i.e. Modus Operandi
- ✓ Copy of FIR
- ✓ Compromised channel's working status – blocked/ unregistered

Bank on its own discretion, may also seek the following details/ documents from the customer to investigate the complaint.

- ✓ Claim Form (Bank will provide the format)
- ✓ Copy of FIR duly attested by Notary Public.
- ✓ An undertaking for loss amount upto Rs.25000/- and Affidavit for and amount above Rs. 25000/- (Bank will provide the format)
- ✓ Copy of a/c Passbook, which shows transactions date, time & amount (Bank Passbook 1st Page & 1 Month statement prior to fraudulent transaction to till date also required)/statement
- ✓ Photo copies of all pages of Passport, if applicable.
- ✓ Translated copy of documents in English duly attested by Notary Public, if the documents are in regional language.

7. Customer's Responsibility:

- Bank will not be under obligation and responsible for loss to the customers due to customer's carelessness in keeping cards, Use ID, login ID, PIN, OTP or other security information and not adhering "Do's and Don'ts" issued by the Bank, until and unless the Bank has been notified by the customer. Bank has already publish Do's and Don'ts for our customers on Bank's corporate website at https://www.bankofbaroda.com/contact-centre.htm

  Bank is also using various modes for educating our customers such as Print / Social/ Electronic Media, Personalized SMS, Email, Push notification, publishing product specific information for safe and secure transactions on corporate website etc.

- The Bank will not be responsible for loss to the customer, if the customer acts fraudulently and /or acts without reasonable care which has resulted in loss. Bank will also not be responsible for loss arising out of loss of cards, login ID, PIN, compromise of password or confidential information until and unless the Bank has been notified of such loss/compromise and Bank has taken steps to prevent its misuse.

- The Bank will not be responsible for loss to the customer, if the customer has not notified his current Mobile number, Address, email ID with his base branch. These updated information is required to Bank to send Transaction Alert / other information to customer.

- Bank has also provided Self-Account blocking feature for customer through various channels. In case of suspicious, unauthorized or fraudulent debit transactions, customers may block account by themselves through various channels as under:

Channels available	**Path for blocking the account**
Bank's Website	https://www.bankofbaroda.in/ → Contact Us please → click Online Account Blocking Portal
bob World Internet	please click on link SELF ACCOUNT BLOCKING
UPI	Open BHIM Baroda Pay App → Account Blocking.
Bob World	Open Bob World App More Self account block
WhatsApp Banking	5.Block Digital Channel / Account (Block) → 1.Account Blocking (Accblk)

8. Facility of Electronic transaction to such customers which have not registered their mobile number in their accounts:

As per the referenced RBI notification “The banks may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank”. Broadly, the electronic banking transactions are divided into two categories:

a. **Face to face / proximity payment transactions** – All these transactions are performed in physical presence of customer based on the two factor authentication.

b. **Remote/ online payment transactions** – All these transactions are performed based on the two factor authentication. Customer who have not registered their mobile number in their account are not able to use Bank’s various applications like bob World, bob World Internet, BHIM Baroda Pay etc. They are also not able to perform E-commerce transaction through bob World Debit as Bank is using OTP authentication as second factor authentication in these transactions.

Hence for registration of any Digital product, mobile number registration is mandatory.

9. Force Majeure:

The Bank shall not be liable to compensate customers for delayed credit, if some unforeseen events (including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters/calamities or other “Acts of God”, Pandemic situation like COVID-19, War, damage to the Bank’s facilities or of its correspondent , no connectivity, absence of the usual means of communication or all types of transportation etc., which are beyond the control of the Bank, prevent the Bank from performing Banking obligations within the specified service delivery parameters.

Annexure – 1

Table -1

Maximum Liability of a customer.
(Fraudulent transaction reported to the Bank within 4 to 7 days)

Type of Account	Maximum Customer Liability
• Basic Saving Bank Deposit accounts	Rs. 5,000/-
• All other SB accounts • Pre-paid payment Instruments and Gift Cards • Current / Cash credit / Overdraft Account of MSMEs • Current Accounts / Cash Credit / Overdraft Account of Individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs. 25 lacs • Credit cards with limit upto Rs. 5 lacs	Rs. 10,000/-
• All other Current / Cash Credit / Overdraft Account • Credit cards with limit above Rs. 5 lacs	Rs. 25,000/-

Table -2

Overall liability of the customer in third party breaches in such Unauthorised Electronic Banking Transactions where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system

Time taken to report the fraudulent transaction from the date of receiving the communication	Customer 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	100% Liability.

Table -3

Current Channels available for blocking of Digital channels namely bob World Debit, bob World, bob World Internet and UPI

Mode of blocking channel	Bank's major Digital Products			
	bob World Debit	**UPI**	**bob World**	**bob World Internet**
Contact Centre (Agents)	Yes	Yes	Yes	Yes
IVR	Yes	Yes	Yes (through Agents)	Yes
Branch (in business hours)	Yes	Yes	Yes	Yes
Mobile Banking	Yes			
Net Banking	Yes			
WhatsApp Banking	Yes	Yes		
SMS Facility		Yes	Yes	
Bob World UPI App		Yes		

Table -4

Current Channels available for registration of customer complaint related to unauthorized Electronic Banking Transactions –

Channel	Availability	Timing
Toll free number through contact centre	24X7	24X7
Bank's Website	24X7	24X7
Bank's Application – bob World and bob World Internet	24X7	24X7
Reporting to Home branch	During the branch banking timing	