ALLAHABAD BANK

Customer Protection–
Limiting Liability of Customers in Unauthorised Banking Transaction

RBI has issued guidelines on "**Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions"** vide their circular bearing no. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017.

On the basis of above guidelines, the Board of Directors have approved the policy on **Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions** for our Bank in its meeting held on 12th December 2017.

The policy is detailed hereunder:

A) Modes of Unauthorised Electronic Banking Transaction (UEBT)

I. The Unauthorised Electronic Banking Transaction (UEBT) may happen by cloning of the card, Data skimming, Phishing, Farming, etc. as under:

a. **Card Skimming**- This is done by use of a device that reads and stores magnetic strip information when a legitimate transaction is conducted. This information is then copied on another card, which is used for the fraudulent transactions. Skimming allows criminals to take possession of cardholder's data stored in the magnetic strip in total which includes the CVV, and other discretionary data. This can be used for fraudulent transactions through the websites in foreign countries where the PIN and Password are not required for carrying out Debit Card transactions.

b. **Point of Sale (PoS) terminals or PIN Entry Device (PED) Tampering** Sometimes merchant swipes for a second time on another swipe device fraudulently on the pretext of recording for loyalty and reward programs. The second swipe may be for obtaining card data for cloning purpose.

c. **Data compromise**- The theft of cardholder data is from issuers, merchants, processors or third party agents, normally via unauthorized server intrusions. Storage of unencrypted cardholder data by these entities facilitates this criminal activity.

PINs are also captured with overlay devices positioned on legitimate unattended terminals, such as ATMs, automated fuel dispensers and also by, shoulder surfing. In addition hidden cameras are often positioned at or near POS terminals in order to capture PINs.

d. **Phishing**- A social engineering scheme where criminals masquerade as a legitimate financial services institution to obtain account data from the cardholder. Phishing is normally conducted via electronic mail, but telephone versions are also common. As data is obtained directly from the cardholder, it normally includes the Personal Identification Number (PIN). This is how,

phishing enables ATM fraud.

e. **Pharming**- A social engineering scheme that is based on redirecting website traffic to another illegitimate site where customers unknowingly enter their personal data.

f. Imprinting of extra (i.e., multiple) transaction receipts by sales personnel.

g. **Malware**- Criminal installs the malware in the ATMs to take control over ATMs which allow stealing data, PINs and cash.

II. **Fake Assistance:** Once these perpetrators spot a target they appear to be very helpful and offer assistance to the unsuspecting cardholder and ask for the basic card details i.e., Card no. PIN, expiry date & CVV. These details are sufficient for fund transfer.

III. **Liability in case of unauthorised transaction in specified scenarios.**

Table-A

Sl. No.	Txn Type	Case Types	Customer Liability	Bank's Liability	Remarks
1	ATM	PIN Shared	Full	Zero	PIN written on card, Kept along with card / shared.
2		Card & PIN given to known person	Full	Zero	Card & PIN given to the family persons, friends or known persons but claimed as fraudulent withdrawal.
3		Card Lost	Full	Zero	Card lost but not informed to the bank and meantime transactions done through the card.
4			Zero	Full	Card lost & informed to bank but bank failed to block the card; transactions done.
5		Card issued without customer request	Zero	Full	Card issued in customer Ac without customer request and txn done.
6	E-Commerce	Card Lost	Full	Zero	Card Lost but had not informed to bank or customer was not aware of it
		OTP Shared	Full	Zero	OTP shared by the customer.
		Card details shared with the unknown persons	Full	Zero	Card details shared over phone/mail to the unknown person.
7	Internet/ Mobile Banking/ UPI	Credential shared	Full	Zero	User credentials or OTP shared by customer.

B) Limitation of Customer's Liability: In case of Unauthorised Electronic Banking Transaction, the liability of customer shall be as under:

a) Zero Liability of a customer

A customer's entitlement to zero liability shall arise where the unauthorised 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 unauthorised transaction.

b) Limited liability in case of reporting beyond 3 working days

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 the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in the undernoted Table whichever is lower:

Case I: Where there is a delay of 4 - 7 working days after receiving the communication from the bank on the part of the customer in notifying the bank of such a transaction.

Case II: Where there is delay in reporting beyond 7 working days, after receiving the communication from the bank on the part of the customer in notifying the bank of such a transaction.

Table-B

Type of Account	Maximum Liability (Rs.)	
	4-7 working days	Beyond 7 working days
• BSBD Accounts	5,000	8,000
• 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	35,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000	1,00,000

C) Unauthorised Electronic Banking Transaction(UEBT) Reporting Channels

The reporting of UEB Transactions will be through following channels:

1. SMS to 9223150150 for Card blocking followed by e-mail/ letter or reporting at the branch
   a) BLOCKCARD<space><last 6 digit of card no.> or
   b) BLOCKACC<space><last 6 digit of Account no.>
2. Toll Free number 1800 220 363
3. Application to the home branch. Applicant should submit FIR copy in case of fraudulent transaction, lost card.
4. Mail to customercare@allahabadbank.in
5. 24x7 Call Centre (when put in place)

D) Burden of Proof

The burden of proving customer liability in case of unauthorised electronic banking

transactions shall lie with the bank.

Operating Procedure for handling UEBT

Actions to be taken:

a) Advise the customer about the SMS channel which blocks transactions of the account or the card instantly.

b) For the information received through reporting channels (Sl. No. 2 - 4) the receiving person has to enter the details in Bank's CGRC System and provide the customer with an acknowledgement for the complaint.

c) The dispute lodged in CGRC are categorized and are to be handled by designated officials at CBSO, Mumbai.

d) The designated official at CBSO will ascertain the customer liability immediately otherwise CBSO will credit (shadow reversal) the amount to the customer's account within 10 working days from the date of such notification by the customer.

e) To ascertain the customer's liability within 90 days from the date of receipt of the complaint, the designated official will have to take up with the concerned bank/branch and collect the details about the UEBT and submit the same to the Zonal / FGMO/ Central Compensation Settlement Committee (CCSC) for timely settlement of the cases.

f) The composition & discretionary authority of the Compensation Settlement Committees will be as under:-

Compensation Settlement Committee at	**Members**	**Discretionary authority**
Zonal Office	Zonal Head CM (P&D) Sr Mgr/ Mgr IT	Rs.50,000/-
FGMO	FGM, AGM/CM (P&D) & CM/ Sr Mgr IT	Rs.1lac
Head Office	GM(P&D), GM(IT), GM(Insp.)	Full

The decisions of the committees would be recorded in writing.

g) The Central Compensation Settlement Committee will take into consideration the recommendations of the FGMO & Zonal Office level Settlement Committees.

h) The CSCs will identify the customer's liability considering above details and following indicators:

- Not blocking the card immediately on knowing about the fraud transaction.
- No action even though SMS alerts of the transactions received in the mobile number registered with the Bank.
- No action even after checking the account balance / statement through Internet Banking / ATM/ branch.

i) The decision of the Central CSC will be implemented by CBSO, Mumbai to dispose of the disputed Unauthorised Electronic Banking Transaction (UEBT) within 90 days from the receipt of the complaint.

j) Publicity:

i) To provide publicity to general public / customers about Table A, Table B and

procedure to report Un-authorised Electronic Banking Transactions should be prominently displayed in bank's premises.

ii) This information may also be sent to all customers through e-mail ids available, displayed in the Bank's Website and may be published in the news papers every 6 months.

Reporting and Monitoring Requirements

- The customer liability cases would be put up to the Standing Committee on customer service and thereafter to the Customer Service Committee of the Board on quarterly basis.
- The reporting shall include volume/ number of cases and the aggregate value involved and distribution across various categories of cases.
- The Standing Committee on Customer Service shall review on quarterly basis the unauthorised 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.
- The reporting and monitoring of customer liability cases will be done by DIT, HO

****