युनाइटेड बैंक ऑफ इंडिया
वैकल्पिक सुपुर्दगी माध्यम विभाग
प्रधान कार्यालय, कोलकाता

United Bank of India
Alternate Delivery Channel Department
Head Office , Kolkata

Annexure - II

POLICY ON LIABILITY SHIFT – UNAUTHORIZED ELECTRONIC BANKING TRANSACTIONS

1. Introduction:

Electronic Banking transactions has been experiencing a surge in the recent past due to various factors like moving to a "less cash society", availability of multiple options to the customers, ease of performing transactions, reliable and fast settlement of transactions with adequate security features.

2. Objective:

The premise of the policy is to define, determine and decide the quantum of compensation, if any, to be paid to the customers in case of reported unauthorized electronic banking transactions.

3. Definition:

Electronic Banking transactions are broadly categorised as under:

(a) Remote / Online payment transactions that does not require presentment of physical payment instruments and which includes internet banking, mobile banking, Card not present transactions and Pre-paid payment instruments like e-wallet.
(b) Proximity payment transactions which require physical payment instrument like Card / Mobile phone to be present at the point of transaction which includes ATM, Point-of-Sales (POS) and payment using Quick Response (QR) code.

4. Procedures:

Electronic banking transactions are enabled with multiple factor authentications. The pre-requisites are transaction authentication is enumerated below:

4.1 Proximity transactions:

(i) **Card based transactions (including prepaid Cards) at ATM, Point-of-Sales (POS) locations**: Availability of the physical card as well as the PIN linked to the card is essential.

(ii) **Through Mobile Banking using QR Code**: The essentials are physical availability of the registered mobile number, activated Application (Mobile Banking / UPI) downloaded on the Mobile and MPIN for the transaction.

4.2 Remote / Online transactions:

(i) **Internet Banking:** The requisites are valid user ID, Login Password, Transaction Password and One Time Password (OTP) sent on the registered mobile number for each transaction.

(ii) **Mobile Banking :** Registered Mobile number, Mobile / UPI Application with application password and MPIN for each transaction are essential.

(iii) **Card Not Present:** These types of transactions are done through e-commerce websites or their applications which are commonly called as MobileApps. The essentials are valid card number, CVV in some sites, Expiry date of the Card and One Time Password (OTP) delivered for each transaction on the registered mobile number.

(iv) **Prepaid instruments like e-wallet:** Login ID which is either the Registered Mobile Number or the registered e-Mail ID and the linked password for the e-wallet account. Wallet transactions are normally limited to restricted payment volumes in terms of number of transactions as well as amount of transactions.

5. Roles and Responsibility

5. 1 Customers' Responsibility:

Maintenance of the credentials like physical card, PIN / MPIN and Passwords in a secured manner and not sharing the One Time Password (OTP) is the responsibility of the customer. Bank will not be responsible due to compromise of the same due to customers' negligence on this aspect. The PIN and passwords are the property of the customer which is never stored at the Bank other than in a universally standard encrypted form.

Customers are required to keep their Mobile hand set in working mode to enable receipt of transaction alerts.

In case of loss of physical card or Mobile handset the Bank has to be notified immediately with a copy of the Police Record like FIR copy / General Dairy report.

5.2 Bank's Responsibility:

5.2.1 - The Bank shall have a secured system of storing the credentials required for electronic banking transactions and in an encrypted form for CVV of Physical Card / passwords / PIN / MPIN.

Any incidence occurring despite the above aspects being proved to be kept as required shall be treated as negligence on other than customer or Bank and shall be treated as third party related incidence.

5.2.2 - The Bank shall have the best available technology for generating and delivery of SMS alerts for all kinds of transactions. However, final delivery of the SMS alert on the registered mobile number of the customer is reliant on external factors like capability of the service provider of the target mobile number; the target mobile number being in working mode, roaming facility being enabled and the handset is in a ready mode to receive the alert so generated.

5.2.3 - Customers shall be provided an alternative / additional facility of delivery of transaction alert on the registered e-mail ID as per specific request of the customers.

6. Reporting Procedure:

For any perceived unauthorized transaction/s, the customer may report about the same through the following modes:

(i) Through a letter to the parent branch where the account resides.

(ii) Through a reply enabled transaction alert sent on the registered mobile or registered e-mail ID if the customer. The reply shall have a provision for reporting of unauthorized as well as failed transactions in a structured format. The format shall contain fields like account number, transaction date and transaction amount for further action at the Bank's end.

(iii) Through grievance link available in the Bank's website.

(iv) Through helpline provided by the Bank.

7. Compensation Details:

(i) In case of negligence on the part of the Customer, the customer has to be replied within 10 days from the date of complaint providing adequate details of the transactions along with sequence of events and sufficient evidence to establish negligence on the part of the customer.

(ii) In case of contributory fraud / negligence / deficiency on the part of the Bank, the amount of unauthorized transactions has to be reversed to the customer's account within 10 days from the date of notification of the same by the customer.

(iii) In case of third party involvement in the unauthorized transactions, the amount reported as unauthorized shall be reversed to the customer's account within 10 days from the date of notification of the same by the customer if the reporting of the same is made by the customer within 3 days after receiving notification of the transactions from the Bank.

(iv) In case of incidences falling under category as stated under (iii) above, and where the reporting is made by the customer between 4 to 7 days of the notification of the transaction from the Bank, the liability of the customer shall be limited to the quantum as stipulated by Reserve Bank of India and as stated hereunder and the remaining amount shall be reversed to the customer's account within 10 days from the date of reporting of the matter by the customer.

Type of Account	**Maximum Liability in Rs**
BSBD Account (No frill accounts)	5,000.00
❖ 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 25.00 lakh ❖ Credit cards with limit up to Rs 5.00 lakh	10,000.00

❖ All other Current / Cash Credit / Overdraft Accounts ❖ Credit cards with limit above Rs 5.00 lakh	25,000.00

(v) In case of incidences falling under category as stated under (iii) above and where the reporting is made by the customer after 7 days of the notification of the transaction from the Bank, the liability of the customer shall be the total sum of the reported transactions. Provided, upon further representation of the customer the matter and quantum of compensation shall be decided as per approval of the Managing Director & Chief Executive Officer of the Bank or in his absence as per approval of the Executive Director of the Bank.

The Compensation details shall be incorporated in the Bank's Compensation Policy for future guidance.

- The number of working days shall be reckoned as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

8. Review of the Policy

The Policy shall be reviewed annually or as and when necessitated as per modified directives received from Reserve Bank of India.

****