Customer Protection Policy

(Unauthorized Electronic Banking Transactions)

Approved by the board in its meeting dated 25th May 2018

INTRODUCTION

Keeping in mind the increasing thrust on financial inclusion & customer protection, the Reserve Bank of India had issued a circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions RBI/2017-18/109-DCBR.BPD.(PCB/RCB).Cir.No.06 /12.05.001/2017-18 on December 14, 2017 which inter-alia requires Banks to formulate a Board approved policy in regard to customer protection and compensation in case of unauthorized electronic banking transactions.

This policy is applicable to individuals/entities that hold savings, current, cash credit, Overdraft & such operative accounts with the bank and seeks to communicate in a fair and transparent manner the Bank's policy on:

a) Customer protection (including mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions),

b) Customer liability in cases of unauthorized electronic banking transactions

c) Customer compensation due to unauthorized electronic banking transactions (within defined timelines)

2. COVERAGE

Broadly, electronic banking transactions can be divided into two categories:

a) 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), etc.)

b) 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.)

This policy covers transactions only through the above modes. The policy excludes electronic banking transactions effected on account of error by a customer (e.g. NEFT,IMPS, RTGS carried out to an incorrect payee or for an incorrect amount), transactions done under duress, claims due to opportunity loss, reputation loss, other incidental costs or collateral damage.

3. SAFEGUARDING CUSTOMER DETAILS

The bank shall take industry standard security measures & mechanisms to safeguard and protect customers from unauthorised transactions. The bank's environment shall be protected with multiple layers of security to allow only need based authenticated access to its systems. All data between the device and the bank's environment is encrypted through use of SSL. Bank provides highly secure option of Challenge-response codes on its netbanking platform through usage of Nexus Tru ID Mobi token. All transactions are secured by 2 factor authentication including SMS OTPs.

The bank subjects its systems through periodic Vulnerability Assessments & Penetration Tests and keeps its systems updated with the latest security updates/patches. Apart from transactions, the bank has a robust alerting mechanism which apart from sending alerts of any changes/events in the account, even alerts customers on login to the netbanking account, through SMS & email. The customer

has option to immediately freeze his Netbanking account by just sending a sms. The bank takes adequate safeguards and keeps on reviewing its security processes at regular intervals.

4. LIMITED LIABILITY OF CUSTOMER

Customer compensation & Liability shall be based as per the following cases:

a) Complete Liability of customer

i) Customer shall bear the entire loss in cases where the loss is due to negligence by the customer, e.g. where the customer has shared payment credentials or Account/Transaction details, viz. Internet Banking user Id & PIN, Debit/Credit Card PIN/OTP or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing / Vishing attack. This could also be due to SIM deactivation by the fraudster.

Under such situations, the customer will bear the entire loss until the customer reports unauthorised transaction to the bank. Any loss occurring after reporting of unauthorised transaction shall be borne by the bank.

ii) In cases where the responsibility for unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere in the system and when there is a delay on the part of the customer in reporting to the Bank beyond 7 working days, the customer would be completely liable for all such transactions.

b) Zero Liability of customer

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

i) Customer shall be entitled to full compensation of outgo from the customer's account in the event of contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether transaction is reported or not, by the customer)

ii) Customer has Zero Liability in all cases of 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 of customer

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

i) In cases where the loss is due to negligence by a customer, such as where he has shared payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised 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 the customer notifies the bank of such a transaction within four to seven working days of receiving a communication of the 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.

Type of Account	Maximum Liability Within 3 working days (Rs.)	Maximum Liability Within 4 to 7 working days (Rs.)
BSBD Accounts	Zero Liability	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 upto Rs. 5 lakh		10,000
All other Current/Cash Credit/Overdraft Accounts		25,000

Any unauthorised electronic banking transaction reported after 7 working days will be treated as 100% customer liability.

5. REVERSAL TIMELINE for ZERO Liability/Limited Liability of customer

On being notified by the customer, the bank shall credit (shadow credit) 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.

Within 90 days of date of reporting, the Bank shall either establish customer negligence or provide final credit to the customer. The credit shall be valued dated to be as of the date of the unauthorised transaction such that in case of a debit card/bank account, the customer shall not suffer loss of interest and in case of credit card, the customer does not bear any additional burden of interest. The Bank may, at its discretion, agree to credit the customer even in case of an established negligence by the customer.

Customer would not be entitled to compensation of loss if any, in case customer does not agree to get the card blocked and/or does not cooperate with the Bank by providing necessary documents including but not limited to police complaint and cardholder dispute form.

6. Roles & Responsibilities of the Bank

a) The Bank will provide the details of the policy with regard to customer liability at the time of opening the accounts. The Bank shall display the approved policy in Bank's website. The policy will also be available at Bank's branches for the reference by customers. The Bank shall also ensure that existing customers are individually informed about the bank's policy through publication on the website and wherever possible, through SMS and email alerts.

b) The Bank will regularly conduct awareness on carrying out safe electronic banking transactions to its customers and staff. Information of Safe Banking practices will be made available on any or all of the following - website, emails, ATMs, net banking, mobile banking. Such information will include rights and obligation of the customers as well as non-disclosure of sensitive information e.g. password, PIN, OTP, date of birth, etc.

c) The Bank shall communicate to its customers to register for SMS alerts. The Bank will send SMS alerts to all valid registered mobile number for all debit electronic banking transactions. The Bank may also send alert by email where email Id has been registered with the Bank.

d) The Bank will enable various modes for reporting of unauthorized transaction by customers. These may include SMS, email, website, Mobile Banking, Netbanking or through its branches.

e) The Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgement. On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account or card.

f) During investigation, in case it is detected that the customer has falsely claimed or disputed a valid transaction, the bank reserves its right to take due preventive action of the same including and not limited to closing the account or blocking card limits

g) The Bank may restrict customer from conducting electronic banking transaction including ATM transaction in case of non-availability of customer's mobile number.

7. Rights & Obligations of the Customer

a) Customer is entitled to

i) SMS alerts on valid registered mobile number for all financial electronic debit transactions
ii) Email alerts where valid email Id is registered for alerts with the Bank
iii) Register complaint through multiple modes – as specified in the clause 'Bank's roles & responsibilities'
iv) acknowledgement of the complaint with Date & time of receipt
v) Receive compensation in line with this policy document where applicable. This would include getting shadow credit within 10 working days from reporting date and final credit within 90 days of reporting date subject to customer fulfilling obligations detailed herein and with customer liability being limited as specified in Table-I

b) Customer is bound by following obligations with respect to banking activities:

i) Customer should compulsorily register his valid mobile number with the Bank.
ii) Customer should preferably register his email ID so as to receive transaction alerts over email, in addition to SMS alerts.
iii) Customer shall immediately update change in his /her registered contact details, as soon as practicable. Bank shall not be liable for non-reporting of transactions on the changed mobile number/email ID, unless the same is registered with the bank. Such failure to update update the Bank with changes shall be considered as customer negligence & unauthorized transaction arising out of this delay shall be treated as customer liability.
iii) Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint and provide copy of the same to the Bank.
iv) Customer should co-operate with the Bank's investigating authorities and provide all assistance.
v) Customer must not share any sensitive information (such as Debit/Credit Card details like card no, expiry date, PIN, CVV, NetBanking Id & password, OTP, transaction PIN, Nexus TruID responses, challenge/security questions & answers) with any entity, including bank staff.
vi) Customer must protect his/her device as per best practices specified on the Bank's website, including updation of latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab)
vii) Customer shall abide by the tips and safeguards mentioned on the Bank's website on Secured Banking.
viii) Customer shall go through various instructions and awareness communication sent by the bank on secured banking
ix) Customer must set transaction limits to ensure minimized exposure.
x) Customer must verify transaction details from time to time in his/her bank statement and/or credit card statement and raise query with the bank as soon as possible, in case of any mismatch.

8. Proof of customer liability:

The Bank has a process of second factor authentication for electronic transactions, as regulated by the Reserve Bank of India. Bank has onus to prove that all logs / proofs / reports for confirming two factor authentication is available. Any unauthorized electronic banking transaction which has been processed post second factor authentication known only to the customer would be considered as sufficient proof of customer's involvement / consent in effecting the transaction.

Reporting & monitoring mechanism

Customer liability cases shall be periodically reviewed in the Executive 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. The Board shall periodically review the unauthorised electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of 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.

Linkage to other Customer Service Polices of the bank

This policy shall be read in conjunction with the Customer Compensation policy and Customer Grievance Redressal policy.

*****