DOHA BANK INDIA BRANCH CUSTOMER PROTECTION POLICY

Published: March 2022

SUMMARY OF ABBREVIATIONS

Abbreviation	Description
ATM	Automated Teller Machine
CVV	Card Verification Value
NEFT	National Electronic Funds Transfer
OTP	One Time Password
PIN	Personal Identification Number
POS	Point of Sale
RBI	Reserve Bank of India
SMS	Short Message Service

TABLE OF CONTENTS

1. POLICY SUMMARY

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 Unauthorized Electronic Banking Transactions. (RBI/2017-18/15 DBR.No. Leg.BC.78/09.07.005/2017-18 dated July 6, 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.

2. PURPOSE

This policy 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)

3. SCOPE

3.1 In case of Doha Bank, Electronic banking transactions usually cover transactions through the below modes:

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 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.)

c) Any other electronic modes of credit effected from one entity to another currently being used or adopted from time to time.

3.2 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 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.

4. APPLICABILITY

4.1 This policy is applicable to entities that hold relationship with the bank viz.:

a) Individual and non-individual customers who hold current or savings account.

b) Individual / non-individual entities that hold debit card.

c) Individual / non-individual entities that use other electronic platforms of the Bank like internet banking, mobile banking.

4.2 This policy is not applicable to:

a) Non-Customer that uses Bank's infrastructure e.g. ATMs, electronic wallet.

b) Entities that are part of the ecosystem such as interchange organizations, Franchises, Intermediaries, Agencies, Service partners, Vendors, Merchants etc.

5. ASPECTS OF CUSTOMER PROTECTION POLICY

5.1 Policy outlines the obligations on behalf of bank and customer to ensure the onus of liability arising out of fraudulent transaction. Bank must ensure following:

a) Appropriate systems and procedures to ensure safety and security of electronic banking transactions.

b) Dealing quickly and empathetically with customer grievances

c) Mandatorily ask customers to register for SMS & wherever available register for E-mail alerts for electronic banking transactions.

d) Mandatorily send SMS and wherever available send E-mail alerts for electronic banking transactions.

e) Advise customers to notify unauthorised electronic banking transactions to Banks instantly upon occurrence.

5.2 Facilitate reporting of unauthorized electronic banking transactions through Phone Banking, website (support section) and Branch network.

a) Ensure immediate acknowledgement of fraud reported by customer.

b) Take immediate steps on receipt of an unauthorised transaction from customer to prevent further damage.

c) If the Bank identifies through external intelligence or during the course of its investigations, that the customer is a repeated offender in reporting fraudulent transactions, then it shall not only declare customer's liability, but also terminate the relationship with due notice.

5.3 Customer must ensure the following:

a) Mandatorily register for SMS & Email alerts at the time of account opening

b) Mandatorily notify the Bank about any change of mobile number, email ID & Communication address

c) Block/hotlist card or account if they suspect any malicious activities or in an event of lost /theft.

d) Customers at any point should not disclose or share account details, number, PIN, CVV with anyone over mail, calls or any other mode of communication.

e) Confidentiality of password for internet banking & mobile banking should be ensured at all times.

f) Customers to ensure passwords are kept secure and not to be recorded on paper or accessible electronic devices.

g) Customer should check the transaction message triggered by bank and report any discrepancy immediately.

h) Customer must submit necessary documentation to the bank as per defined timelines else the case stands closed under customer liability.

i) Statement of account should be checked regularly and discrepancy if any should be reported to the Bank immediately.

j) Passbook issued if any should be updated from time to time.

k) Crossed / account payee cheques should be issued as far as possible.

l) Blank cheques should not be signed and customers should not record their specimen signature either on passbook or cheque book

m) PIN & passwords should be changed on a regular basis.

6. POINTS COVERED UNDER THE POLICY

Customer shall be compensated in line with this policy in case of loss occurring due to unauthorized transaction as follows:

6.1 Zero Liability of customer

a) Customer shall be entitled to full compensation of real loss in the event of contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer)

b) 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 unauthorized transaction.

6.2 Limited Liability of customer

a) Liability in case of financial losses due to unauthorized electronic transactions where responsibility for such transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and

b) There is a delay on the part of customer in notifying/reporting to the Bank beyond 3 working days and less than or equal to 7 working days (after receiving the intimation from the Bank), the liability of the customer per transaction shall be limited to transaction value or amounts mentioned in Annexure -1 whichever is lower.

6.3 Complete Liability of Customer

a) 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/ 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.

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

c) 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.

6.4 Other Points

a) The Bank shall afford shadow credit to the customer account within 10 working days from the date of reporting in all cases as per above statements. Within 90 days of date of reporting, the Bank shall either establish customer negligence or provide final credit to customer. Customer will be given value dated credit (based on date of unauthorized transaction) when customer becomes eligible to be compensated. In case of debit card/ bank account, the customer shall not suffer loss of interest

b) The Bank may, at its discretion, agree to credit the customer even in case of an established negligence by the customer.

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

d) Compensation would be limited to real loss after deduction of reversals or recoveries received by the customer.

7. THIRD PARTY BREACH

The following would be considered as Third-party breach where deficiency lies neither with the Bank nor customer but elsewhere in the system:

a) Application frauds

b) Account takeover

c) Skimming / cloning

d) External frauds / compromise of other systems, for e.g. ATMs / mail servers etc. being compromised.

8. ROLES & RESPONSIBILITIES OF THE BANK

8.1 The Bank shall ensure that the Customer protection policy is available on the Bank's website as well as 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.

8.2 The customers will be advised to notify the Bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction and informed that the longer the time taken to notify the Bank, the higher will be the risk of loss to the Bank/ customers. To facilitate this, the Bank will provide customers with 24x7 access through multiple channels (at a minimum, via website, SMS, e-mail, call center support, reporting to home branch, etc.).

8.3 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 through campaigns on any or all of the following - website, emails, ATMs, phone banking, 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.

8.4 The Bank shall communicate to its customers to mandatorily 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.

8.5 The Bank will enable various modes for reporting of unauthorized transaction by customers. These may include SMS, email, website, Phone Banking or through its branches. The Bank will also enable specific space on its home page where customers can report unauthorized electronic banking transaction

8.6 The Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgement specifying complaint number, date and time of transaction alert sent and date and time of receipt of customer's notification. On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account or card.

8.7 The Bank shall ensure that all such complaints are resolved and liability of customer if any, established within a maximum of 90 days from the date of receipt of complaint, failing which, bank would pay compensation as described in Annexure 1.

8.8 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 closing the account or blocking card limits.

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

8.10 This policy should be read in conjunction with Grievance Redressal Policy of the Bank. Clauses from the Bank's Grievance Redressal Policy shall form a part of this policy where not specifically addressed in this policy.

9. RIGHTS & OBLIGATIONS OF THE CUSTOMER

9.1 Customer is entitled to

a) SMS alerts on valid registered mobile number for all financial electronic debit transactions

b) Email alerts where valid email Id is registered for alerts with the Bank.

c) Register complaint through multiple modes – as specified in point relating to Bank's roles & responsibilities.

d) Intimation at valid registered email/ mobile number with complaint number and date & time of complaint

e) 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 Annexure-I.

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

a) Customer shall mandatorily register valid mobile number with the Bank.

b) Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known email/ mobile number. Any failure of customer to update the Bank with changes shall be considered as customer negligence. Any unauthorized transaction arising out of this delay shall be treated as customer liability.

c) 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.

d) Customer should co-operate with the Bank's investigating authorities and provide all assistance.

e) Customer must not share sensitive information (such as Debit/ Card details & PIN, CVV, Net Banking Id & password, OTP, transaction PIN, challenge questions) with any entity, including bank staff.

f) Customer must protect his/her device as per best practices specified on the Bank's website, including updating of latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab)

g) Customer shall abide by the tips and safeguards mentioned on the Bank's website.

h) Customer shall go through various instructions and awareness communication sent by the bank on secured banking.

i) Customer must set transaction limits to ensure minimized exposure.

j) Customer must verify transaction details from time to time in his/her bank statement and raise query with the bank as soon as possible in case of any mismatch.

k) In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorized transaction to the Bank. Any loss occurring after the reporting of the unauthorized transaction shall be accepted by the Bank.

l) The Bank will display the details of the policy in regard to customers' liability in public domain for wider dissemination. The existing customers will also be individually informed about the Bank's policy.

10. NOTIFYING THE BANK OF THE UNAUTHORIZED TRANSACTION

10.1 Customer shall report unauthorized transaction to the Bank at the earliest, with basic details such as Customer ID and/ or Card number (last 4 digits), date & time of transaction and amount of transaction

10.2 Customer shall follow bank's reporting process viz.

a) Notify/ report through the options listed in the section on Roles & responsibilities of Bank (8.4). In case customer is unable to do so, customer could report through phone banking or at the nearest branch.

b) Lodge police complaint and maintain copy of the same and furnish police complaint when sought by bank's authorized personnel.

10.3 Customer shall authorize the bank to block the / debit card/ net banking/ account(s) to reduce likelihood of additional loss

10.4 Customer to clearly specify the facilities to be blocked failing which the Bank reserves the right to block all electronic transactions of the customer to protect the customer's interest. Also, revoking these blocks would require explicit consent from customer for each facility.

10.5 Customer shall share relevant documents as needed for investigation or insurance claim viz. cardholder dispute form, copy of passport in case of international transactions and police complaint.

10.6 Fully co-operate and comply with Bank's reasonable requirements towards investigation and provide details of transaction, customer presence, etc.

11. 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 authentications 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.

12. FORCE MAJEURE

The bank shall not be liable to compensate customers for delayed credit if some unforeseen event (including but not limited to civil commotion, sabotage, lockout, strike or other labor disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents it from performing its obligations within the specified service delivery parameters.

13. ANNEXURE

Unauthorized Transaction due to Bank's negligence	
Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	Customer's Maximum Liability (Rs.)
Customer to report as soon as possible to prevent future losses	Zero Liability
Unauthorized Transaction due to Customer's negligence	
Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	Customer's Maximum Liability (Rs.)
Customer to report as soon as possible to prevent future losses	100% liability till it is reported to Bank

Maximum Liability of a Customer in case of unauthorized Electronic Transaction where Responsibility is neither with the Bank nor with the customer but lies elsewhere in the system & customer has reported unauthorized transaction from transaction date within working days specified in following table:

Type of Account	Within 3 working days (Rs.)	Within 4 to 7 working days (Rs.)
All SB accounts	Zero Liability	10000
Current accounts		10000

Note: As per RBI Guidelines, Maximum liability of customers of Small Accounts / Basic Saving Bank Deposit (BSBD) accounts would not exceed INR 5000/-.

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

END OF DOCUMENT