# DHANERA MERCANTILE CO-OPERATIVE BANK LTD.

## Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions

**Policy 2025-26**

APPROVED BY BOARD OF DIRECTORS

| | |
|---|---|
| **Policy No.** | 3 |
| **Policy Name** | **Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions** |
| **Version No.** | 3.0 |
| **Board Resolution Date** | 28-03-2025 |
| **Board Resolution Number** | 14 |
| **Review Date** | 28-03-2025 |
| **Next review date** | 31-03-2026<br><br>(or earlier if there are any changes) |
| **Classification** | Confidential for Internal Circulation only |

**Version Control Information:**

| Version No. | Date Issued | Author | Update Information |
|---|---|---|---|
| 3.0 | 28-03-2025 | IT Department | Second Published version |
| | | | |

## Background

Customer centricity is one of the five core values of the bank. The Bank truly believes that Customer Experience is the key to keeping customers happy and thereby ensuring a long-lasting relationship with the Bank. Dhanera Mercantile Co-Operative Bank's Customer Protection Policy has been formulated in line with regulator guidelines on Customer Protection – Limiting Liability of Customers in unauthorized Electronic Banking Transactions. Policy outlines the framework for addressing & handling customer grievances related to unauthorized transactions to their accounts /cards and the criteria for determining the customer liability in these circumstances.

The Bank shall ensure that the policy is made available in public domain (Bank's website & Branches).

## Objective

RBI vide its circular dated 14th December, 2017 no. DCBR.BPD. (PCB/RCB).Cir.No.06/ 12.05.001/2017- 18 has issued guidelines on "Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions"

The objective of the policy is to ensure that the systems and procedures in banks are designed to make customers feel safe and define customer liability while carrying out electronic banking transactions.

- Robust and dynamic fraud detection and prevention mechanism
- Appropriate measures to mitigate risks and protect themselves against liabilities arising thereon
- A system to educate customers in protecting themselves from frauds arising from electronic banking & payments

## Coverage of the policy

Electronic banking transactions are divided into two categories:

1. 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 (credit or a debit card), Pre-paid Payment Instruments (PPI) & UPI
2. Face-to-face/ proximity payment transactions (transactions which require physical payment instrument such as a card (includes credit, debit or any prepaid instrument including Forex card) or mobile phone to be present at the point of transaction, e.g., ATM, POS, etc.)

**Aspects of Customer protection policy**

Policy outlines the obligations on behalf of bank and customer to ensure the onus of liability arising out of fraudulent transactions.

***The Bank must ensure following:***

i. Appropriate systems and procedures to ensure safety and security of electronic banking transactions
ii. Dealing quickly and empathetically with customer grievances
iii. Making registration for SMS compulsory for electronic banking transaction
iv. Mandatorily send SMS and wherever available send E-mail alerts for electronic banking transactions
v. Advise customers to notify unauthorized electronic banking transactions to Banks instantly upon occurrence
vi. Facilitate reporting of unauthorized electronic banking transactions through Mobile Banking, website (support section) IVR (dedicated helpline) and Branch network
vii. Ensure immediate acknowledgement of fraud reported by customer
viii. Take immediate steps on receipt of an unauthorized transaction from customer to prevent further damage Like Blocking of Card/s, De-Active of Mobile Banking facility, Freezing of A/c, etc.
ix. 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.

***Customer must ensure the following:***

I. Mandatorily register for SMS & Email alerts at the time of account opening
II. Mandatorily notify the Bank about any change of mobile number, email ID & communication address
III. Block/hotlist card or account or digital payment channels like UPI, Mobile Banking, Internet Banking etc. if they suspect any malicious activities or in an event of lost /theft to avoid further misuse
IV. Customers at any point should not disclose or share account details, card number, PIN, CVV, MPIN, UPI PIN with anyone over mail, calls or any other mode of communication
V. Confidentiality of password for mobile banking should be ensured at all times.
VI. Customers to ensure passwords are kept secure and not to be recorded on paper or accessible electronic devices
VII. Customer should check the transaction message triggered by bank and report any discrepancy immediately
VIII. Customer must submit necessary documentation to the bank as per defined timelines else the case stands closed under customer liability
IX. Statement of account should be checked regularly and discrepancy if any should be reported to the Bank immediately
X. Passbook issued if any should be updated from time to time
XI. Crossed / account payee cheques should be issued as far as possible

XII. Blank cheques should not be signed, and customers should not record their specimen signature either on pass book or cheque book

XIII. PIN & passwords should be changed on a regular basis

XIV. In case of any queries, customer shall email to banks authorized email id (dmcb.ho@dmcbank.in) and/or call to banks authorised helpline numbers (02748-221667). Other authorised contact details of the Bank/Branch are available on banks website https://dmcbank.in

**Burden of Proof of Customer Liability**

- The burden of proving Customer liability in case of unauthorized electronic banking transactions shall be with the bank.

- Bank has implemented process of second factor authentication for electronic transactions, as regulated by the Reserve Bank of India. Therefore, Bank has onus to prove that all logs / proofs / reports for confirming two factor authentications are 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.

- Bank may advise the Customer to file police complaint in case of unauthorised transactions. In such cases Customers shall fully co-operate with Bank and Police authorities or any enforcement authorities for filing compliant / FIR, disclosing all true & fair facts and without hiding any facts.

- During investigation, in case it is detected that the customer has falsely claimed or disputed valid transactions, the bank reserves its right to take due preventive action of the same including closing the account or limiting Electronic Transactions, etc.

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

- Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank shall 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.

- Customer shall provide all necessary documentation as required by the bank to conduct the investigation, for determining customer liability for compensating the customer.

- Customer shall be co-operate with the Bank's investigating authorities and provide all assistance.

**Table 1: Defining Customer Liability**

| Zero customer liability | Limited customer liability # |
|---|---|
| Negligence/ deficiency on the part of the bank (Irrespective of whether or not the transaction is reported by the customer) | a) Loss due to negligence of a customer by sharing payment credentials will be borne by the customer till the time he reports the unauthorized transaction to the Bank.<br><br>b) Loss occurring after reporting of unauthorized transaction to the Bank, shall be borne by the Bank<br><br>c) If the investigation establishes that the transaction is 2 factor authenticated liability of such transactions lies with customer, burden of proof lies with the bank |
| **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. | a) Cases where the responsibility for the 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 of **4 to 7 working days** on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or amount mentioned in table 2 whichever is lower<br><br>b) If the delay in reporting is beyond **seven working days**, the customer liability shall be determined as per the bank's Board approved policy. |

*# Including other scenarios subject to fulfilment of certain terms and conditions*

****Third party breaches:** Third party breaches would cover following unauthorized transactions without customer knowledge

1. ***SIM duplication*** – Cloning of original SIM to create duplicate SIM
2. ***Application related frauds*** – Stolen customer identity which is used to avail banks product & services
3. ***Account takeover*** – Theft of account information to obtain banks products and services including extracting funds from the customers bank account
4. ***Skimming/Cloning*** – Collect data from the magnetic strip of the card and copying the information onto another plastic
5. ***Vendor related frauds*** - Frauds committed by vendors engaged by the Bank

**Table 2: Maximum Liability of a Customer under paragraph 7 (ii)**

<table>
<tr><th>Time taken to report the fraudulent transaction from the date of receiving the communication</th><th colspan="3">Customer's liability (₹)</th></tr>
<tr><td>Within 3 working days</td><td colspan="3">Zero Liability</td></tr>
<tr><td>Within 4 to 7 working days</td><td colspan="3">All other SB accounts<br>Type of Account Maximum Liability ( ₹ )</td></tr>
<tr><td></td><td>BSBD Accounts</td><td>5,000</td></tr>
<tr><td></td><td>All other SB accounts<br>Prepaid Instruments & Gift Cards/ Forex Cards/ Current/ Cash Credit/ OD accts. of MSMEs Current Account/ Cash Credit/OD accts 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</td><td>10,000</td></tr>
<tr><td></td><td>Current/ Cash Credit/OD accounts, Credit Cards with limit above Rs. 5 lacs</td><td>25,000</td></tr>
<tr><td>Beyond 7 working days</td><td colspan="3">Full Liability<br>However, customer to be compensated up to a limit of Rs.5000/- or the transaction value, whichever is lower, only once in the lifetime of the account as per Bank's Board approved compensation policy.</td></tr>
</table>

The number of working days mentioned in Table 2 shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

**Table 2: Summary of a Customer under paragraph 7 (ii)**

| **Time taken to report the fraudulent transaction from the date of receiving the communication** | **Customer's 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 | MD and CEO and / or General Manager are empowered to determine on case to case basis. |

**Reversal Timeline for Zero Liability / Limited Liability of Customer**

**On being notified by the customer, the bank shall credit (shadow reversal) 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 (without waiting for settlement of insurance claim, if any). The credit shall be value dated to be as of the date of the unauthorised transaction.**

Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. In such cases, the detailed note for such a case would be put up before MD and CEO and / or General Manager for reimbursement to the Customer if any. Board / Executive Committee shall be informed about total number of cases periodically, also action taken thereon, the functioning of the grievance Redressal mechanism and take appropriate measures to improve the system and procedures.

However, in the case of failed electronic banking transactions, the terms of payment of customer compensation and TAT for such payment shall strictly be in accordance with provisions of RBI Cir. DPSS.CO.PD No.629/ 02.01.014/2019-20 dated September 20, 2019 on "Harmonization of Turn Around Time (TAT) and customer compensation for failed transactions using authorized Payment Systems" as laid down in the said circular.

In case of NFS ATM transaction, as per NPCI NFS OC – 317 dt.24th December 2018 EMV Liability Shift process, Bank is raising EMV Counterfeit Chargeback against acquirer bank and recover the loss amount. The TAT for Compliance or Acceptance of Chargeback from acquirer bank is 28 Calendar days. Hence, Bank shall wait for 28 days to give the clear credit in customer account.

This policy document is placed before the Board of Directors and unanimously passed in its meeting held on 28-03-2025 vide board resolution no. 14.

## Certified Copy By

**For, Dhanera Mercantile Co-Operative Bank Ltd.**

**Manager/CEO**

**Place: Dhanera**