The Nasik Merchants Co-op Bank Ltd.

Customer Protection Policy 2026-27

By

Accounts Department

Accounts Department

Customer Protection Policy (Unauthorized Electronic Banking Transactions)

I. POLICY APPROVAL.

Resolved in BoD Meeting.	
Date	Resolution No
27/03/2026	32

II. PERIOD OF POLICY.

Period of Policy.
With effective from 01/04/2026 and will be reviewed every year in the month of March. However, will be modified, changed as & when needed.

III. SIGN OFF.

Shri. Gurappa Savkar Assistant General Manager Chief Accountant	
Shri. Santosh Jadhav Chief Compliance Officer	
Shri. Trigun Kulkarni, Chief Executive Officer	

IV. Distribution.

01	All Branches
02	All HODs at HO

Accounts Department

Customer Protection Policy (Unauthorized Electronic Banking Transactions)

Table of Contents

Accounts Department

Customer Protection Policy (Unauthorized Electronic Banking Transactions)

01. INTRODUCTION.

01.01. 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 of Co-operative Banks in Unauthorized Electronic Banking Transactions, bearing No. RBI/DOR/2025-26/292 DOR.MSC.REC.No.211/01-01-037/2025-26 dated November 28 2025(Responsible business conduct Direction, 2025) which inter-alia requires Bank to formulate a policy in regard to customer protection and compensation in case of unauthorized electronicbanking transactions.

01.02. With surge in Digital transactions across the Banking industry, the associated risks have also multiplied and hence Customer protection against unauthorized electronic banking transactions has assumed greater importance from the regulatory perspective.

01.03. Accordingly, this policy is designed duly incorporating the systems and procedures to make Customersfeel safe while carrying out electronic banking transactions. It includes the following:

01.03.01. Appropriate systems and procedures to ensure safety and security of electronic transactions carried out by customers.

01.03.02. Accurate and dynamic fraud detection and prevention mechanism.

01.03.03. Mechanism to assess the risks of gaps in the bank's existing systems which result in unauthorized transactions and measure the liabilities arising out of such events.

01.03.04. Appropriate measures to mitigate the risks.

01.03.05. System of customer education so as to protect themselves from electronic banking and payments related frauds.

02. OBJECTS OF THE POLICY.

02.03. Customer protection, including mechanism of creating customer awareness on therisks and responsibilities involved in electronic banking transactions.

02.04. Customer liability in cases of unauthorized electronic banking transactions.

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

02.06. Bank ensures :-

02.06.01. To take industry level standard security measures & mechanisms to safeguard and protect customers from unauthorized transactions.

02.06.02. That the bank's environment shall be protected with multiple layers of security to allow only need based authenticated access to its systems.

02.06.03. That all data between the device and the bank's environment is encrypted. All transactions are secured by 2 factor authentication including SMS OTPs.

02.06.04. That the bank subjects its systems through periodic Vulnerability Assessments & Penetration Tests and keeps its systems updated with the latest security updates/patches.

02.06.05. That 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 net banking account, through SMS & email.

03. COVERAGE OF THE POLICY.

03.03. Customers conducting electronic banking transactions using the bank's infrastructure viz. ATM, Cash recycler or bank's Digital channels viz. Mobile banking, Internet banking etc. or other bank's infrastructure viz. ATM, POS, UPI app, Bank's app etc. Broadly, electronic banking transactions can be divided into two categories:

03.03.01. Remote/ online payment transactions where transactions do not require physical payment instruments to be presented at the point of transactions e.g. internet banking, mobile banking, card notpresent (CNP) transactions, Pre-paid Payment Instruments (PPI), etc.

03.03.02. Face-to-face / proximity payment transactions, where 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.

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

03.05. Guidelines for determining the Customer's liability for unauthorized electronic banking transactions, its compensation and creating customer awareness on the risks and responsibilities involved in electronic banking transactions.

04. SCOPE.

04.03. This policy is applicable to individuals / entities that hold savings, current, cash credit, Overdraft & such operative accounts with the bank.

05. PHRASEOLOGY / LEXICON.

05.01. ABBREVIATIONS.

05.01.01. RBI = Reserve Bank of India

05.01.02. UPI = Unified Payment Interface.

05.01.03. PIN = Personal Identification Number.

05.01.04. QR = Quick Response.

05.01.05. POS = Point of Sale.

05.01.06. OTP =One Time Password.

05.02. DEFINATIONS.

05.02.01. "Information" means information regarding the money or other relevant particulars relating to customer, or any User, or the Account or any Transaction.

05.02.02. "PIN" means a Personal Identification Number, a numeric code generated by customer to access the banking services post login into mobile banking app and/orUPI app and/or execute any financial or non-financial transaction or to access banking services via debit card at ATM or any similar device.

05.02.03. "Password" means an alphanumeric code generated by the customer to access the banking services post login into internet banking portal and/or execute any financial or non-financial transaction.

05.02.04. "Point of Sale/ POS Transactions" means transactions initiated at Merchants' point of sale terminals.

05.02.05. "Transaction" means any transaction or instruction effected or issued, or purported to be effected or issued, by customer through the mobile banking, Internet Banking, UPI, by use of Debit Card etc.

05.02.06. "OTP" means an automatically generated numeric or alphanumeric string of characters that authenticates the customer for a single transaction.

05.02.07. "Fraudulent transaction" means a transaction unauthorized by the customer or account holder of bank.

05.02.08. "Hacking" means gaining of unauthorized access to data in a system or computer.

05.02.09. "Skimming" means a method used by fraudulent individual to capture financialinformation from typically a debit / credit card holder.

05.02.10. "Phishing" refers to fraudulent activity that attempts to obtain sensitive information over the internet.

05.02.11. "Smishing" means a type of social engineering attack that uses text messages inorder to deceive recipients.

05.02.12. "Vishing" means the fraudulent activity of making phone calls in order to induceindividuals to reveal financial information.

05.02.13. "Electronic banking transactions" means remote / online payment transactions, such as transactions that do not require physical payment instruments to be presented at the point of transactions e. g. Internet banking, mobile banking, UPI, Prepaid instruments, online transactions through card (Card not present) etc.

conducted by the Customer other than from the branch channel and also face-to-face/ proximity payment transactions, such as transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transactions i.e. ATM, POS, QR Scan & Pay etc.

05.02.14. "Working days means" the number of working days shall be counted as per the working schedule of the home/nearest branch of the Customer excluding the date of receiving the communication.

06. TRANSACTION ALERTS.

06.01. Bank would ask customers to mandatorily register for SMS alerts and wherever available, register for e-mail alerts.

06.02. SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.

06.03. Bank would not provide electronic channels for customers not having their mobile number registered with the bank.

06.04. Bank would periodically educate customers via SMS/ e-mails to notify bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction and make them aware that the longer the time taken to notify the bank, the higher will be the risk of loss to them.

07. REPORTING OF UNAUTHORIZED ELECTRONIC BANKING TRANSACTIONS BY CUSTOMERS.

07.01. Bank will provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking (call center), SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to Home branches etc.) for reporting unauthorized transactions that have taken place and/ or loss or theft of payment instrument such as card, etc.

07.02. Bank shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any.

07.03. Additionally, a direct link for lodging the complaints with specific option to report unauthorized electronic banking transactions will be provided by the bank on home page of the website.

07.04. Bank shall also implement a loss/ fraud reporting system to ensure that immediate response/ auto-response is sent to the customers acknowledging the complaint along with the registered complaint number and would also record the date & time of the message and receipt of customer's response if any.

07.05. Bank may explore any alternative channel for receiving complaints from customers as per the business case.

08. THIRD PARTY BREACH.

The Bank will consider as Third-party breach where deficiency lies neither with the Bank nor with the customer but elsewhere in the system, such as-

08.01. Application frauds.

08.02. Hacking

08.03. Account takeover

08.04. Skimming / cloning

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

09. ZERO LIABILITY OF THE CUSTOMER.

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

09.01. Contributory fraud/ negligence/ deficiency on the part of the bank, irrespective of whether or not the transaction is reported by the customer.

09.02. 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.

Accounts Department

10. LIMITED LIABILITY OF THE CUSTOMER.

A Customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:

10.01. In cases where the loss is due to negligence by a customer, such as where he hasshared 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 borne by the bank.

10.02. In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere inthe system and the customer notifies the bank of such a transaction within four to seven working days of receiving the communication from the Bank, the per transaction liability of the customer shall be limited to the transaction value or the amount as under:-

10.02.01. For Basic Savings deposit account: - Maximum liability of Rs 5,000 or transaction values whichever islower.

10.02.02. For 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 lakhs / Credit cards with limit up to Rs.05.00 lakhs:- Maximum liability of Rs 10,000.00 or transaction value whichever islower.

10.02.03. All other Current/ Cash Credit/ Overdraft Accounts:- Maximum liability of Rs 25,000 or transaction values whichever islower.

10.03. In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere inthe system and the customer notifies the bank of such a transaction after seven working days of receiving the communication from the Bank, it will be treated as 100% customer liability.

11. COMPLETE LIABILITY OF THE CUSTOMER.

11.01. 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 & Password, mobile banking PIN, UPI PIN, Debit / Credit Card details including Card number, expiry month & year, CVV, Card PIN / OTP or any other critical information through whichfraudster may onboard / execute any transaction on any electronic channel or dueto improper protection on customer devices like mobile / laptop/ desktop leading tomalware / Trojan or Phishing / Vishing / smishing 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 unauthorized transaction to the bank.

11.02. 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 seven working days, the customer would be completely 100% liable for all suchtransactions.

Table 3
Summary of Customer's Liability

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	As per BANK's Board approved policy

Accounts Department

12. REVERSAL TIMELINE FOR ZERO LIABILITY/ LIMITED LIABILITY OF THE CUSTOMER.

12.01. On being notified by the customer, the bank shall credit (shadow reversal – lien) the amount involved in the unauthorized 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.

12.02. The credit shall be value dated to be as of the date of the unauthorized transaction.

12.03. Banks may also at their discretion decide to waive off any customer liability in caseof unauthorized electronic banking transactions even in cases of customer negligence.

12.04. Customer's complaint shall be resolved and post determining the liability of the customer, the customer is compensated (removing the lien) within 90 days from the date of receipt of the complaint.

12.05. If the complaint is not resolved or customer liability is not determined, the bank shall compensate the customer (removing the lien) not exceeding 90 days from the date of receipt of the complaint as per the schedule mentioned earlier in the policy.

12.06. In case of debit card/ bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

13. BURDEN OF PROOF OF CUSTOMER LIABILITY.

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

13.02. Bank has a process of second factor authentication for electronic transactions, as regulated by the Reserve Bank of India.

13.03. The Onus to prove all logs / proofs / reports are availability of two factor authentication is on the bank.

13.04. Any unauthorized electronic banking transaction which has been processed post second factor authentication known only to the customer, would be considered assufficient proof of customer's involvement / consent in effecting the transaction.

14. INSURANCE COVER.

Bank shall cover its liability by taking adequate insurance cover either through its Bankers indemnity policy, card protection policy or through any cyber insurance policy,if available.

15. ROLES & RESPONSIBILITIES OF THE BANK.

15.01. Bank shall ensure that this policy is available on the Bank's website as well as at Bank's branches for customer reference.

15.02. 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 or any alternative channel.

15.03. Bank shall communicate to its customers to mandatorily register their mobile number for receiving SMS alerts and e-mail notifications wherever e-mail id is registered.

15.04. Bank will enable various modes for reporting of unauthorized transaction by customers.

15.05. Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgement specifying complaint number, date and time oftransaction alert sent and date and time of receipt of customer's notification.

15.06. On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account or card.

15.07. Bank shall ensure that all such complaints are resolved and liability of customer ifany, established within a maximum of 90 days from the date of receipt of complaint.

15.08. 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 blocking card limits.

15.09. Bank may restrict customer from conducting any electronic banking transaction including ATM

transaction in case of non-availability of customer's mobile number.

15.10. This policy will be read in conjunction with Grievance Redressal Policy and Customer Compensation Policy of the Bank.

16. DUTIES & OBLIGATIONS OF THE CUSTOMER.

16.01. Customer shall mandatorily register valid mobile number with the Bank and even e-mail id wherever available with them.

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

16.03. Bank will only reach out to customer at the last known email/ mobile number.

16.04. Any failure of customer to update the Bank with changes shall be considered as customer negligence.

16.05. Any unauthorized transaction arising out of aforesaid delay shall be treated as customer liability.

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

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

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

16.09. 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 or any other similar device).

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

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

16.12. 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.

17. REPORTING AND MONITORING.

17.01. Branch Manager will report the cases of unauthorized electronic banking transactions to the HOD, IT Department, who will put further to CEO.

17.02. CEO will then place suitably in Committee of Board and the Board.

17.03. 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.

17.04. HOD, IT / The CEO / Committee of Board and the Board shall periodically review the unauthorized 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.

17.05. All such transactions shall be reviewed by the bank's internal auditors.

17.06. Dispensation / Exception:

17.06.01. Dispensation to be sought from Head of Department – IT for any deviations to customer on adequate business justification and approval by the CEO and further ratification of Committee of Board and the Board.

18. REVIEW.

18.01. The policy shall be reviewed once in years or earlier, in the event significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. Procedures and Processes will be reviewed and updated accordingly.

18.02. There has been no change in the Customer Protection Policy this year compared to last year.

********** END ********** END **********