Document Name	Customer Protection Policy	Document Number	OPR/CPP/1.0
Security Classification	Public	Document Status	
Date of Release		Version Number	1.1

Customer Protection Policy – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions

THE NAINITAL BANK LIMITED

Regd. Office: G.B. Pant Road, Nainital.

Uttarakhand

Table of Contents

Document Name	Customer Protection Policy	Document Number	OPR/CPP/1.0
Security Classification	Public	Document Status	
Date of Release		Version Number	1.1

1. Preamble

With the increased thrust on financial inclusion and customer protection and considering the recent surge in customer grievances relating to unauthorized transactions resulting in debits to their accounts/ cards, the criteria for determining the customer liability in these circumstances have been reviewed for electronic banking transaction. Taking into account the risk arising out of unauthorized debits to customer accounts owing to customer negligence/Bank Negligence/banking system frauds/third party breaches and to protect and safeguard the customer interest, keeping in view the guidelines issued by RBI through circular no. DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 issued by the Reserve Bank of India, Bank has formulated Customer Protection Policy for unauthorized electronic Banking transactions reported by customers. Accordingly, the Customer Protection Policy for unauthorized electronic Banking transactions reported by customers has been prepared which covers, the liability of customers in different scenarios. For all such transactions, the Bank would be governed by the Board Approved Customer Protection Policy.

2. Objective

The objective of this policy is to define the rights and obligations of customers and maximum liability of the customer in case of unauthorized electronic banking transaction with emphasis on educating customer about risk arising out of unauthorized transaction and to make customer feel safe about carrying out electronic banking transaction which is essential not only to attract new customer but to retain existing ones.

3. Scope

The policy covers Procedural guidelines to be followed by branches, regions, ATM Cell and Head Office in case of perpetration of frauds in customer's account, establishment of frauds, timely restoration and follow up for expeditious restoration of amount in customer's account and/or recovery of the restored amount.

4. Policy

1. Electronic Banking Transaction:

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

i. 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), and

ii. 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.)

The systems and procedures in bank are designed to make customers feel safe about carrying out electronic banking transactions. To achieve this bank has put in place:

i. appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
ii. robust and dynamic fraud detection and prevention mechanism;
iii. mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorised transactions and measure the liabilities arising out of such events;
iv. appropriate measures to mitigate the risks and protect themselves against the liabilities arising there from; and
v. a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

2. Compensation to Customer

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

Zero Liability of customer

- Customer shall be entitled to full compensation of 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)
- 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 about unauthorised transaction within three working days of receiving the communication from the bank regarding such transactions.

Limited Liability of customer

- 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

- 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),

Complete Liability of customer

- 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 unauthorized transaction to the bank. Any loss occurring after reporting of unauthorized transaction shall be borne by the bank.

- 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.

3. Reporting of unauthorized transactions by customers to banks

Branches must ask customers to mandatorily register for SMS alerts and for e-mail alerts (wherever available), for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.

The customers must be advised to notify their bank of any unauthorised 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/ customer.

To facilitate this, banks has provided customers access through multiple channels which include, via website, e-mail, dedicated toll-free helpline, reporting to home branch, etc. and 24X7 dedicated customer care centre.

Complaints can be registered preferably through Feedback/grievance redressal portal on website of the bank at https://www.nainitalbank.co.in/english/FedbackForm.aspx or through above mentioned channels.

The bank may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank.

4. Immediate Action to be taken by branch and ATM Cell and further follow up taken on detection of fraud.

On receipt of report of an unauthorised transaction from the customer, banks must take immediate steps to prevent further unauthorised transactions in the account:

i. The Digital channel has to be immediately blocked/de-registered from where the digital transaction has happened with the consent of the customer so that the subsequent fraud attack on particular account can be protected and liability of future fraud can be protected after notifying by the customer.

ii. The Bank will notify that the digital channel has been blocked/de-registered from where the

digital transaction has happened preferable through email and or SMS.

5. Guidelines to be followed by Bank to determining the Liability of Customers in unauthorized Electronic Banking Transactions:

a) Zero Liability of a Customer

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

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

ii. 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 a 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 the 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 when there is a delay (of **four to seven working days** after receiving the communication from the bank) 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 the amount mentioned in Table 1, whichever is lower.

Table 1

Maximum Liability of a Customer

Type of Account	**Maximum liability (₹)**
• BSBD Accounts	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 up to Rs.5 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000

Further, if the delay in reporting is beyond **seven working days**, the customer liability shall be determined as per the bank's Board approved policy. Branches shall provide the details of this policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts. Bank shall display their approved policy in public domain for wider dissemination through its website. The existing customers must also be individually informed about the bank's policy.
Overall liability of the customer in third party breaches, as detailed in Point 4.a.ii and 4.b.ii above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised in the Table 2:

Table 2	
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

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.

6. Rights and Obligation of Customer in case of unauthorized electronic Banking Transactions:

Scenario 1: Customer Negligence- Unauthorized Electronic Banking transaction happened due to customer negligence (where customers has shared the payment credentials)

Customer Liability	100% customer Liability
Customer Rights	Customer has to bear entire loss until he/she reports the unauthorized transaction to bank. Any loss occurring after the reporting has to be borne by the bank.
Customer Obligation	Approach the bank as soon as the customer becomes aware of the unauthorized debit. Customer has to be vigilant while doing electronic banking transactions.

The ATM Cell will check the customer negligence based on following parameters and to put it to channel head for approval before communicating same to the customer:

Debit Card Transaction:

1. ATM Cash withdrawal and other POS Transaction: Digital evidence related to use of physical

Debit Card and PIN for the cash withdrawal and POS transaction, status of delivery of transaction alert/OTP and other SMS sent by the bank.

2. E-commerce and other OTP based transaction: Checking the status of OTP delivery.
3. Analysis of EJ log
4. Content of FIR Report
5. Content of Customer Letter
6. Analysis of time of reporting fraud and time of transaction.
7. Analysis of card blocking
8. CCTV footage: as and when required not mandatory for all cases.

Online Banking Transaction:

1. Digital evidence related to use of customer handset, mobile number and mobile application Login/ Transaction PIN.
2. Status of delivery of transaction alert/OTP and other SMS send by the bank.
3. Content of FIR
4. Content of Customer letter
5. Analysis of time of reporting fraud and time of transaction

Scenario 2: Bank' Negligence- Unauthorized Electronic Banking Transaction happened due to Contributory fraud/negligence/deficiency on part of the bank (either committed by the bank staff or bank vendor) - irrespective of whether or not transaction is reported by customer)

Customer Liability	Zero customer Liability
Customer Rights	Customer is having right to get compensation from Bank
Customer Obligation	Customer is required to check the SMS/email alert sent by the bank and approach the bank as soon as the customer becomes aware of the unauthorized debit.

Scenario 3: Third Party Breach- Unauthorized Electronic Banking Transaction happened due to third party breach.

Customer Liability	Based on time taken by customer to report the fraudulent transactions from date of receiving the

	banks communication
Customer Rights	In such cases where the deficiency lies neither with the bank nor with the customer but elsewhere in the system and the customer has notified the bank within seven working days of the transaction, customer is having right to get compensation from bank as per table 1 & 2. In such case where customer has notified the unauthorized transaction to bank after 7 days, bank will have no liability and bank will try to pass the customer claim through Bank's Insurance Agency on best effort basis.
Customer Obligation	Customer is required to check the SMS/email alert sent by the bank and approach the bank as soon as the customer becomes aware of the unauthorized debit.

Reversal Timeline for Zero Liability/ Limited Liability of customer

If customer is eligible for compensation in scenario 2 & 3 then bank will follow the reversal timeline will be applicable as per Point No. 5 of Compensation Policy of the bank.

7. Information/Documents required for resolving the complaint in respect of unauthorized Electronic banking transaction:

From Customers:

- Channel Details like channel name, location etc.
- Transaction details like transaction type, account, date, amount etc.
- Claim Form
- Copy of FIR duly attested by Notary Public

- Undertaking for loss amount up to Rs. 25000/- and affidavit for amount above Rs. 25000/-
- Letter of customer reporting the branch about the fraud.
- Copy of account statement one month prior to fraudulent transaction till date

From ATM Cell:

- SMS Alert details
- Electronic Channels Logs/EJ

All complaints received from the customer in respect of unauthorized electronic transaction will be handled centrally by ATM Cell. After receiving compliant from customer for unauthorized electronic banking transaction, bank will take action as mentioned in table below:

S.No.	Issue	Responsibility	Period of completion of the task

1.	Acknowledgement of Customer Complaint about unauthorized electronic banking transaction.	Branch/ATM Cell	T day
2.	Blocking of the channel after getting confirmation from customer	Branch/ATM Cell	T working Day
3.	Forwarding of complaint to ATM Cell	Branch	T+1 Working day
4.	Communication to customer to provide details required for resolution of complaints	Branch/ATM Cell	T+2 working day (the timeline of resolution will start on submission of all details required for resolution of complaints
5.	Collection of digital records like transaction alert logs, electronic channels logs/EJ to ascertain the negligence of the bank or customer	ATM Cell	T+5 working days
6.	Investigation of unauthorized transaction to determine the extent of customer liability	ATM Cell	T+7 Working days
7.	Reply of complaint to customer providing date of shadow reversal of the amount involved in unauthorized electronic banking transaction in case where customer negligence is not found	ATM cell	T+8 working days
8.	Reply of customer complaints in cases where bank found customer negligence along with justification	ATM Cell	T+8 Working days
9.	Intimation of shadow reversal to customer with the details of document required to bank to get the claim from insurance company	ATM Cell	T+8 working days

	and to clear the unauthorized transaction amount to the customer account		
10.	Submission of claim to Insurance company after getting details/ documents from the customer	ATM Cell	T+30 Working days
11.	Examination of staff accountability and the loop holes in the process	IT department in coordination with Operations and Services Department	T+60 Working days
12.	Investigation of unauthorized Debit Cases	Operations and Services Department	T+60 working days
13.	Submission to restoration proposal to the higher authorities in such cases where bank is liable to compensate the customer and didn't receive the claim or received short claim from insurance company.	ATM cell	T+70 working days
14.	Release of credit to customer account	ATM Cell	T+85 working days
15.	Review of cases where banks has decided to take back the amount credit in customer account as shadow reversal or where bank has rejected the customer complaint and customer is not satisfied with the justification given by the bank	Internal Ombudsman	T+85 working days

To ensure timely compensation to customer in unauthorized electronic banking transaction, Chief Operating Officer will authorize to compensate the customer or in such cases where Banking Ombudsman or any other regulatory agency has given advisory or passed award. For cases beyond the power of Chief Operating Officer, Committee of Executives will decide the issue/compensation amount subject to post facto reportingthe details of the case to MCB.

8. Facility of electronic transaction to such customers which have not registered their mobile numbers in their accounts:

The bank does not provide facility of electronic transactions other than ATM cash withdrawal and POS transaction to customer who does not provide their mobile numbers. In such case customer has to present physically for dong the transaction.

9. Strengthening of system and procedures:

Bank shall provide various options to customer to report unauthorized electronic banking transaction and develop the mechanism to measure the liability arising out of such events. In addition bank shall educate its customer about protecting themselves from frauds through various modes like website, SMS, Notification, advertisement and fake calls with stringent focus on not sharing of PIN, OTP and CVV to anyone including bank officials.

10. Fraud and Risk Management Guidelines

Reporting of frauds to various authorities and as per our Bank's extant guidelines.

11. Reporting

The ATM Cell will submit a monthly statement to board showing status of unauthorized electronic baking transaction reported by customer and the amount paid by the bank in such cases.

Operation and Services Department will report these transactions to Standing Committee on customer service with Root Cause Analysis keeping in view following points

- Similar Nature of Frauds in various cases
- Staff accountability for any unauthorized electronic banking transaction
- Any contributory fraud/negligence/deficiency on the part of the bank.
- Lacuna/weakness in the system and procedure, if any.

The same is also appraised to Customer Service Committee of the board.

12. Staff Accountability:

Central Internal Audit Division of the bank will ascertain staff accountability in such cases where Bank has incurred losses due to negligence on the part of the staff.

13. Customer Responsibility:

- Bank will not be under any obligation and responsible for any loss to the customer due to customer's carelessness in keeping cards, User Id, Login Id, PIN, OTP, or other security information and not adhering to "Do's and Don'ts" issued by the bank until and unless bank has been notified by the customer.
- Bank will not be responsible for loss to the customers if the customer acts fraudulently and/or acts without reasonable care which has resulted in loss. Bank will also not be responsible for loss arising out of loss of cards, login ID, PIN, compromise of password or confidential information until and unless Bank has been notified of such loss/compromise and banks has taken steps to prevent its misuse.
- Bank will not be responsible for loss to the customer, if the customer has not notified his current mobile number, Address, email ID with his base branch. This updated information is required by the bank to send transaction alerts/other information to customer.

14. 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 labour disturbances, accident, fires, natural disasters or other "Act 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.

5. Applicability

The policy is effective from 01st March 2025.

6. Periodicity of Review of Policy

The policy will be valid up to 28th February, 2026. Any directive/ guidelines issued by RBI in this regard shall automatically be part of this policy, during the currency of this policy. The Chairman & CEO may allow continuation of the policy for a maximum period of six months from due date of review, in case the policy cannot be reviewed on or before due date.

End of Document