Document Name	Customer Protection Policy	Document Number	OPR/CPP/2.0
Security Classification	Public	Document Status	Board Approved
Date of Release	March 01, 2023	Version Number	2.0

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

1. Electronic Banking Transaction: 3
2. Rights and Obligation of Customer in case of unauthorized electronic Banking Transactions: 4
3. Dispute Resolution Process –Notifying the bank with respect of Unauthorized Electronic Banking Transactions: 5
4. Reversal Timeline for Zero Liability/ Limited Liability of customer: 8

- 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. 9
- The Bank, at its discretion and in circumstances so prevailing may, agree to credit the customer even in case of an established negligence by the customer 9
- 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 and evidences including but not limited to police complaint and cardholder dispute form 9
- Compensation would be limited to real loss after deduction of reversals or recoveries received by the customer. 9

5. Customer Responsibility: 9
6. Facility of electronic transaction to such customers which have not registered their mobile numbers in their accounts: 9
7. Burden of Proof of customer liability: 10
8. Reporting and Monitoring: 10
9. Staff Accountability: 10

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. 10

10. Force Majeure: 11

Annexure - I 11

Document Name	Customer Protection Policy	Document Number	OPR/CPP/2.0
Security Classification	Public	Document Status	Board Approved
Date of Release	March 01, 2023	Version Number	2.0

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 banks must be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, banks must 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. 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– card number, expiry date, OTP, clicked on unknown links etc.)

Customer Liability	100% of the unauthorized electronic banking transaction amount will be customer Liability and this will be notified to the customer as response to the customer complain and the complaint will be treated as closed
Customer Rights	Customer has to bear entire loss until he/she reports the unauthorized transaction to bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank if the channel or product wherein the unauthorized electronic banking transaction occurred has not been blocked or no action initiated 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.

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 which is limited upto the value date transaction amount of the unauthorized electronic banking transaction
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 for blocking the channel or deregistering from the compromised product. Customer is required to lodge a complaint with the bank. Various mode for lodging / registering customer complaint related to unauthorized electronic banking channels are mentioned in Table 3 of Annexure I .

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

Customer Liability	Customer Liability will be ascertained based on time taken by customer to report the unauthorized electronic banking transaction .
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 which is limited to value date unauthorized electronic banking transaction amount as per Table 1 & 2 in Annexure I . 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.

3. Dispute Resolution Process –Notifying the bank with respect of Unauthorized Electronic Banking Transactions:

The customers must immediately report the 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, bank has provided customers access through multiple channels which include, via website, e-mail, 24*7 dedicated toll-free helpline, reporting to home branch, etc.

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.

The timeline for resolving all such complaint will be 90 days from the date of receipt of the complaint. Customer is required to provide details to report the unauthorized transactions:

- Channel Details like channel name, location etc.
- Transaction details like transaction type, account, date, amount etc.
- Fraud incident details i.e. Modus of Operandi.
- Copy of FIR.

Bank on its own discretion, may also seek the following details / documents from the customer to investigate the complaint

- 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.

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	Branch/ATM Cell	T day

	electronic banking transaction.		
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 and to clear the unauthorized transaction amount to the	ATM Cell	T+8 working days

	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.

4. Reversal Timeline for Zero Liability/ Limited Liability of customer:

- 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.

- The Bank, at its discretion and in circumstances so prevailing may, 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 hot listed or does not cooperate with the Bank by providing necessary documents and evidences including but not limited to police complaint and cardholder dispute form.

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

5. 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.

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

As per the RBI notification "The banks may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank ". However, looking to the customer convenience and the following security feature available in these electronic channels. Bank has decided to allow all Electronic transactions to such customers.

1) Face to face / proximity payment transactions – All these transactions are performed based on the two factor authentication. In all such transactions (like ATM Cash Withdrawal, POS transactions, QR code based transaction) customer is required to present physical payment instrument (card or Mobile number) and their credential like PIN, Biometric etc.

2) Remote / Online payment transactions – All these transactions are performed based on the two factor authentication. Customer who have not registered their mobile number in their account are not able to use mobile based application like UPI, BHIM etc. They are also not able to perform E-commerce transactions through Debit Cards as Bank is using OTP authentication as second factor authentication in these transactions.

3) Hence for registration of any Digital product, mobile number registration is recommended.

7. Burden of Proof of customer liability:

The burden of proving customer liability in case of unauthorized electronic banking transactions shall lie on the bank. 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.

8. Reporting and Monitoring:

Operation & Services Department shall report the customer liability cases to the Customer Service Committee of the Board every Quarter. 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 Standing Committee on Customer Service in the bank shall periodically review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redress mechanism and take appropriate measures to improve the systems and procedures. All such transactions shall be reviewed by the bank's internal auditors.

9. 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.

10. 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.

Annexure - I

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 (₹)**
• Basic Small Basic Deposit 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	10,000
• All other Current/ Cash Credit/ Overdraft Accounts	25,000

Overall liability of the customer in third party breaches in such Unauthorized Electronic Banking Transactions 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	100 % Liability

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 3
Channels available for registration of customer complaint related to unauthorized Electronic banking transactions

Channel	**Availability**	**Available during**	**Timing**
24 X 7 Toll free Number (1800 180 4031)	Yes	24 x 7	24 x 7
Website (through grievance Redressal Portal)	Yes	24 x 7	24 x 7
Reporting to Home Branch	Yes	During the branch banking timing	

5. Applicability

The policy is effective from 01st March, 2023

6. Periodicity of Review of Policy

The policy will be valid upto 28th February, 2024. Any directive/ guidelines issued by RBI in this regard shall automatically be part of this policy, during the currency of this policy. The MD & 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