North East Small Finance Bank

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

Effective Date	24-08-2018
Approver	Board of Directors
Approved on	24-08-2018
Policy Owner	Head- Liability
Review frequency	Annual

Version History

Version	Date	Author(s)	Summary of Changes
1.0	19.05.2018	Sudip Choudhury	Document Created

Review Record

Version	Date	Reviewer(s)	Designation	Department
1.0	20.08.2018	Mr. Pranjal Medhi	Head Liability	Business
	20.08.2018	Mr. Mukesh Singh	Chief Compliance Officer & Company Secretary	Compliance

Table of content:

1. Preface :

North East Small Finance Banks (NESFB) has always laid special emphasis on Financial Inclusion and on customer protection. In line with its mission & vision and the applicable regulatory guidelines, this policy intends to put in place the guidelines for Customer Protection in case of an event of an unauthorized electronic transaction in the customer's account. The policy also aims to determine the customer's and the Bank's liability under such circumstances.

2. Objective:

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:

The electronic banking transaction can be broadly classified into two categories

Remote/Online payment transaction (payment instrument not present).
Face to Face/ Proximity payment transaction (transaction with the physical payment instrument)

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, card not present (CNP) transactions, Pre-paid Payment Instruments (PPI), 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. 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:

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

i) Individual and non-individual customers who hold current or savings account. ii) Individual / non-individual entities that hold credit card and/or prepaid card.

iii) Individual / non-individual entities that use other electronic platforms of the Bank like internet banking, net banking and wallet. b) This policy is not applicable to:

i) Non-Customer those of them use Bank's infrastructure e.g. ATMs, electronic wallet

ii) Entities that are part of the ecosystem such as Interchange organisations, Franchises, Intermediaries, Agencies, Service partners, Vendors, Merchants etc.

5. 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

6. Definitions & Explanations:

(for the purpose of this policy)

a) Real loss is defined as financial outgo from customer's account e.g. debit to customer's account or card.

b) Card not present (CNP) transactions are defined as transactions that require use of Card information without card being physically used e.g. e-commerce transactions

c) Card present (CP) transactions are defined as transactions that require use of physical card e.g. at ATM or shops (POS)

d) Payment transactions are defined as transactions that involve transfer of funds from one account/ wallet to another electronically and do not require card information e.g. NEFT

e) Unauthorized transaction is defined as debit to customer's account without customer's consent

f) Consent includes authorization of a transaction debit either through standing instructions, as per accepted banking practice and regulation, based on account opening process and related matters or based on additional authentication required by

the bank such as use of security passwords, input of dynamic password (OTP) or static VBV/ MCSC, challenge questions or use of Card details (CVV/ Expiry date) or any other electronic authentication option provided by the Bank.

g) Date & time of reporting is defined as date & time on which customer has submitted a unique complaint. Date of receiving communication from the Bank, is excluded for purpose of computing number of working days for all action specified in this policy. The working schedule of the home branch would be considered for calculating working days for customer reporting. Time of reporting will be as per Indian Standard Time.

h) Notification means an act of the customer reporting unauthorized electronic banking transaction to the bank

i) Number of days will be computed based on working days

j) Mode of reporting will be the channel through which customer complaint is received first time by the Bank, independent of multiple reporting of the same unauthorized transaction. k) Loss in foreign currency if any shall be converted to Indian currency for the purpose of this policy as per bank's policies on conversion at card rate net of commission.

7. Responsibility of the Bank:

Bank shall ensure that all the customers on boarded are compulsorily registered for SMS alerts and wherever available, register the customers email address for mail alerts for electronic transactions. SMS and email alert (when email address is available) shall be sent to customers mandatorily. The customer will be advised to notify the bank of any unauthorized transactions at the earliest, post occurrence. To facilitate the reporting of such incident , NESFB shall provide a 24x7 access through multiple channels like website, Integrated Voice Response (IVR), a dedicated toll free helpline number, reporting at branches. NESFB will also put in place a link in the website for such reporting any such unauthorized transaction, which shall evoke an immediate auto response acknowledging the complaint & providing a complaint registration number.

NESFB shall take the utmost care to widely publicize the available channels to the customers and undertake an endeavor in educating the customers that delay in reporting of unauthorized transactions results in higher loss to the bank and customer. NESFB on

receipt of any incidence of unauthorized transaction, shall immediately take action to prevent any further transaction in the account or channel.

NESFB shall maintain a system in place, which will record the date & time of all the alerts sent to customers. NESFB shall not provide such electronic channels to customers who do not provide their mobile numbers to the bank.

8. Liability of the customer:

Customer Zero liability	Fraud/ negligence/deficiency on the part of the bank, whether reported or not by the customer.
	Third party breach, where the deficiency is neither with the NESFB or customer but elsewhere. And the customer informs the bank within three working days of receiving the communication/ alert from the bank regarding such unauthorized transaction.
Customer Limited liability	Loss arising due to negligence of the customer, by sharing payment credentials. Customer will bear the entire loss. However any loss arising post reporting to the bank, shall be borne by the bank.
	Loss arising on unauthorized transactions, where the reason can be attributed to neither the customer nor bank but elsewhere in a system & the customer delays the reporting by four to seven working days, the liability shall be as per below mentioned Table 1

Table 1

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

Delay in reporting beyond 7 days, shall be reviewed in the Customer Standing Committee meeting, and finalize the maximum liability in case where neither the customer nor the bank is at fault i.e. Third-party Breach.

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	To be taken up in the Customer Standing Committee Meeting.

9. Timelines for all reversals:

The number of days to be considered is the number of working days of the base branch excluding the date of receipt of the notice. NESFB shall credit the liability amount as specified above within 10 working days in shadow balance in value date. NESFB shall reverse all liability credits with value dates, so that the customer does not incur any loss of interest.

NESFB shall ensure that the complaints, such received, shall be resolved completely within a maximum of 90 days from the date of the receipt. If any exceptional event where the complaint could not be resolved within 90 days, it shall be referred to the Customer Standing Committee. The Committee shall also consider all such complaints received, whether closed or not, with total bifurcations on channels, amounts, modes, geographical spread etc. in total.

10. Policy Review & Updates

This Board approved policy will be reviewed as and when required or at least on an annual basis for incorporating changes and regulatory updates, if any, in overall grievance redressal mechanism, to improve customer experience and satisfaction.

11. Regulatory References

1. Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. Circular no RBI/2017-18/15 DBR.No.Leg. BC.78/09.07.005/2017-18
2. RBI Master Circular on Customer Service in Banks dated July 1, 2015
3. IBA Model Policy for Grievance Redressal in Banks
4. IBA Fair Practice Code
5. IBA Fair Practice on Lending
6. IBA Model Customer Rights Policy
7. BCSBI Code of Commitment to Customers