The Kangra Co-Operative Bank

Customer Protection Policy (Unauthorized Electronic Banking Transactions)

(Approved by the Board at its meeting held on 17.03.2024)

1. Introduction:

With the increased thrust on financial inclusion, customer protection, and considering the recent surge in customer grievances relating to unauthorized transactions, the criteria for determining the customer liability in these circumstances have been reviewed for electronic banking transactions.

Taking into account the risks arising out of unauthorized debits to customer accounts owing to customer negligence / Bank negligence / banking system frauds / third party breaches, the rights and obligations of customers in case of unauthorized transactions in specified scenarios, are reviewed. Guideline for the same is given by RBI, in notification DBR.No.Leg.BC.78/09.07.005/2017-18 dated 6th July 2017 in respect of Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking transactions

2. Objective of the Policy:

This policy document aims to make customer more confident against the risks arising out of unauthorized debits to customer accounts owing to customer negligence / Bank negligence / banking system frauds / third party breaches and to clearly define the rights and obligations of customers in case of unauthorized transactions in specified scenarios to use electronic banking transactions and defined the maximum customer liability for the electronic banking transactions to make customers feel safe about carrying out electronic banking transactions.

The Bank believes that providing the protection to the customer against unauthorized electronic transactions is a boon to customer service to make customers feel safe about carrying out electronic banking transactions and which is essential not only to attract new customers, but also to retain existing ones.

3. Scope/Coverage:

Electronic Banking Transactions generally covers transactions through following modes-

i) Remote/ Online Payment Transaction (e.g. Mobile Banking, Card not present Transactions, Internet Banking, Pre Paid Payment Instruments etc.)
ii) Face to Face/ Proximity Transaction (e.g. ATM, POS, QR code based transactions etc.)
iii) Any other transaction done by electronic mode and accepted by the Bank for debiting/crediting customer account.

4. Right and Obligation of customer in case of unauthorized electronic banking transaction in specified scenario:

i) **Scenario 1**: Customer Negligence - Unauthorized Electronic Banking Transaction happened due to customer negligence (such as where he has shared the payment credentials – card number, expiry period, 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 complaint and the complaint will be treated as closed by the Bank.

Customer Right – Customer to bear the entire loss of the transaction until he / she reports the unauthorized electronic banking transaction to the bank/ / branch etc. Any loss (up to the value dated transaction amount) 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 is required to be vigilant while doing electronic banking transaction.

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

Customer Liability – Zero Liability

Customer Right – In such cases where customer has suffered loss due to Contributory fraud / negligence / deficiency on the part of Banks, Customer is having right to get compensation from Bank which is limited up to the value date transaction amount of the unauthorized electronic banking transaction.

Customer Obligation – Customer is required to check the SMS / Email alert sent by 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 needs to lodge the complaint with the bank. Various mode for lodging/ registering customer complaint related to unauthorized Electronic Banking Channels are mentioned in Table 3 of Annexure 1.

iii) **Scenario 3:** Third Party Breach - Unauthorized Electronic Banking Transaction happened due to Third Party breach:

Customer Liability – Customer Liability will be ascertained based on the time taken by the customer to report the unauthorized electronic banking transaction as per Table 1 & Table 2 mentioned in Annexure 1

Customer Right – In such cases where customer has suffered loss due to third party breach where the deficiency lies neither with the Bank nor with the customer but lies elsewhere in the system, and the customer has notified the Bank **within seven working days**. Customer is having the right to get the compensation from Bank, which is limited upto the value date unauthorized electronic banking transaction amount as per Table 1 & Table 2 of Annexure 1. In such cases where customer has notified the unauthorized transaction to Bank after 7 days, Bank will have no liability, and this will suitably be communicated to the customer. Bank will try to

pass the customer claim through Bank's Insurance Agency for that channel if available on best effort basis.

Customer Obligation – Customer is required to check the SMS / Email alert/ account statement and approach the Bank as soon as the customer becomes aware of the unauthorized electronic banking transaction debit.

5. Dispute Resolution Process- Notifying the Bank in respect of Unauthorized Electronic Banking transaction:

i) Customer is required to immediately report the unauthorized electronic banking transaction through various channels provided by the Bank and displayed at Bank website.

ii) On receipt customer's complaint (notification), Bank will take immediate steps to prevent further unauthorized transaction in the account and by blocking/ deregistering customer from notified electronic channel.

iii) The timeline for resolving all such complaint will be 90 days from the date of receipt of the complaint. Customer is required to provide following details to report the unauthorized transaction-

- ✓ Channel details like channel name, location etc.
- ✓ Transaction details like transaction type, account, date, amount etc.
- ✓ Fraud incident details i.e. Modus Operandi
- ✓ Copy of FIR
- ✓ Compromised channel's working status – blocked/ unregistered

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

- ✓ Claim Form (Bank will provide the format)
- ✓ Copy of FIR duly attested by Notary Public.
- ✓ An undertaking for loss amount upto Rs.25000/- and Affidavit for and amount above Rs. 25000/- (Bank will provide the format)
- ✓ Copy of a/c Passbook, which shows transactions date, time & amount (Bank Passbook 1st Page & 1 Month statement prior to fraudulent transaction to till date also required)/statement
- ✓ Photo copies of all pages of Passport, if applicable.
- ✓ Translated copy of documents in English duly attested by Notary Public, if the documents are in regional language.

6. Customer's Responsibility:

- Bank will not be under obligation and responsible for loss to the customers due to customer's carelessness in keeping cards, Use ID, login ID, PIN, OTP or other security information and not adhering "Do's and Don'ts" issued by the Bank, until and unless the Bank has been notified by the customer. Bank has already publish Do's and Don'ts for our customers on Bank's corporate website at https://www.kangrabank.com

  Bank is also using various modes for educating our customers such as Print / Social/ Electronic Media, Personalized SMS, publishing product specific information for safe and secure transactions on corporate website etc.

- The Bank will not be responsible for loss to the customer, 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 the Bank has been notified of such loss/compromise and Bank has taken steps to prevent its misuse.
- The 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 to Bank to send Transaction Alert / other information to customer.

7. Facility of Electronic transaction to such customers which have not registered their mobile number 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 features available in these electronic channels, bank may allow electronic transactions to such customers.

a. **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 transaction, QR code based transaction) customer is required to present physical payment instrument (Card or Mobile number) and their credential like PIN, Biometric etc.

b. **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 Bank's various Mobile based Applications. They are also not able to perform E-commerce transaction through Debit cards as Bank is using OTP authentication as second factor authentication in these transactions.

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

8. Force Majeure:

The Bank shall not be liable to compensate customers for delayed credit, if some unforeseen events (including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters/calamities or other "Acts of God", war, damage to the Bank's facilities or of its correspondent , Bank's lack of connectivity, absence of the usual means of communication or all types of transportation etc., which are beyond the control of the Bank, prevent the Bank from performing Banking obligations within the specified service delivery parameters.

Annexure – 1

Table -1
Maximum Liability of a customer.
(Fraudulent transaction reported to the Bank within 4 to 7 days)

Type of Account	Maximum Customer Liability
• Basic Saving Bank Deposit accounts	Rs. 5,000/-
• All other SB accounts • Pre-paid payment Instruments • Current / Overdraft Account of MSMEs • Current Accounts Overdraft Account ofIndividuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs. 25 lacs	Rs. 10,000/-
• All other Current / Overdraft Account	Rs. 25,000/-

Table -2
Overall liability of the customer in third party breaches in such Unauthorised Electronic Banking Transactions where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system

Time taken to report the fraudulent transaction from the date of receiving the communication	Customer 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.

Table 3
Current Channels available for registration of customer complaint related to unauthorized Electronic Banking Transactions –

Channel	Availability	Available during	Timing	Auto Response
SMS	No	No	No	No
Customer care number	Yes	24X7	24X7	No
Website	Yes	24X7	24X7	No
IVR	No	No	No	No
Reporting to branch	Yes	During the branch banking timing		No