Annexure -A

THE KANGRA CENTRAL CO-OPERATIVE BANK LTD.
कांगड़ा केन्द्रीय सहकारी बैंक सीमित
Head Office, Civil Lines, Dharamshala, Distt. Kangra, H.P. - 176 215, Ph:01892-223280, 224607

POLICY ON CUSTOMER PROTECTION – LIMITING LIABILITY

Approved by the BOD in its meeting dated 21.10.2023

The Kangra Central Cooperative Bank Ltd Head Office, Dharamsala-176215

TABLE OF CONTENTS

(Approved by the BOD in its meeting dated 21.10.2023)

1. Introduction:

The Kangra Central Cooperative Bank Ltd, is committed to provide superior and safe customer service experience to all its customers. Bank has over the years invested in technology and has robust security systems and fraud detection and prevention mechanisms in place to ensure safe and secure banking experience to its customers.

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 in Unauthorized Electronic Banking Transactions. (RBI / 2017 – 18 / 15 DBR. No. Leg. BC. 78 / 09.07.005 /2017 - 18 dated July 6, 2017) which inter-alia requires Banks to formulate a Board approved policy in regard to customer protection and compensation in case of unauthorized electronic banking transactions

2. Objective:

This policy seeks to communicate in a fair and transparent manner the Bank's policy on:

- Customer protection (including mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions),
- Customer liability in cases of unauthorized electronic banking transactions
- Customer compensation due to unauthorized electronic banking transactions (within defined timelines)

3. Scope:

Electronic banking transactions usually cover transactions through the below modes:

- 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.)
- 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.)
- Any other electronic mode of credit effected from one entity to another currently being used or adopted from time to time

This policy covers transactions only through the above modes. It 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.:

- Individual and non-individual entities who hold current or savings account or credit facilities.
- Individual / non-individual entities that hold ATM debit card / Rupay KCC debit Card

- Individual / non-individual entities that use other electronic platforms of the Bank like internet banking, mobile banking and UPI

B. This policy is not applicable to:

- Non-Customer that use Bank's infrastructure e.g. ATMs, electronic e-wallet
- Entities that are part of the ecosystem such as Interchange Organizations, Franchises, Intermediaries, Agencies, Service partners, Vendors, Merchants etc.

5. Definitions & Explanations: (for the purpose of this policy)

- Real loss is defined as financial outgo from customer's account e.g. debit to customer's account or card.
- 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.
- Card present (CP) transactions are defined as transactions that require use of physical card e.g. at ATM or shops (POS)
- Payment transactions are defined as transactions that involve transfer of funds from one account/ e-wallet to another electronically and do not require card information e.g. NEFT.
- Unauthorized transaction is defined as debit to customer's account without customer's consent
- 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.
- 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.
- Notification means an act of the customer reporting unauthorized electronic banking transaction to the bank
- Number of days will be computed based on working days of the parent branch.
- 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.

6. Points covered under the policy:

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

A. Zero Liability of customer

- Customer shall be entitled to full compensation of real 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 within three working days of receiving the communication from the bank regarding the unauthorized transaction.

B. 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).The liability of the customer per transaction shall be limited to transaction value or amounts mentioned in Annexure -1 whichever is lower.

C. 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 etc. This could also be due to SIM duplication 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.
- Customer will be fully liable for the loss where he has not opted for SMS alert facility.

D. Other Points

- Any complaint / claim, no matter the date of reporting shall be considered valid only after submission of all documents to the bank. Customer will be given 50 days' time from date of reporting for submission of documents. In cases where customer negligence is not observed, the Bank shall afford amount on hold credit to the customer account within 10 working days from the date of receipt of all documents.In cases where prima facia, customer negligence is evident, no amount on hold credit will be provided. If the investigation proves negligence in cases where amount on hold credit is already given, Bank will reverse the amount.
- Within 90 days of date of submission of documents, 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 may, at its discretion, 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 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.

7. 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:

- Application frauds
- Account takeover
- Skimming / cloning
- External frauds / compromise of other systems, for e.g. ATMs / mail servers etc. being compromised

8. Roles & Responsibilities of the Bank:

(a) The Bank shall ensure that the Customer protection policy is available on the Bank's website as well as at Bank's branches for the reference by customers. The Bank shall also ensure that existing customers are individually informed about the bank's policy through SMS or other mode.

(b) The 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. Such information will include rights and obligation of the customers such as non-disclosure of sensitive information. e.g. password, PIN, OTP, date of birth, etc.

(c) The Bank shall communicate to its customers to mandatorily register for SMS alerts. The Bank will send SMS alerts to all valid registered mobile number for all debit electronic banking transactions. The Bank may also send alert by email where email Id has been registered with the Bank.

(d)The Bank will enable various modes for reporting of unauthorized transaction by customers. These may include SMS, email, website, toll free number, IVR, Phone Banking or through its branches. The Bank will also enable specific space on its home page where customers can report unauthorized electronic banking transaction

(e)The Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgement. On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account or card.

THE K.C.C. BANK LTD. H.O. Dharamshala

(f)The Bank shall ensure that all such complaints are resolved and liability of customer if any, established within a maximum of 90 days from the date of receipt of complaint, failing which, bank would pay compensation as described in Annexure 1.

(g)During investigation, in case it is detected that the customer has falsely claimed or disputed a valid transactions, the bank reserves its right to take due preventive action of the same including closing the account or blocking card .

(h)The Bank may restrict customer from conducting electronic banking transaction including ATM transaction in case of non-availability of customer's mobile number.

(i)This policy should be read in conjunction with Grievance Redressal Policy of the Bank. Clauses from the Bank's Grievance Redressal Policy shall form a part of this policy where not specifically addressed in this policy. The policy to be made available on Bank's Web-site.

9. Rights & Obligations of the Customer

A. Customer is entitled to

- SMS alerts on valid registered mobile number for all financial electronic debit transactions.
- Email alerts where valid email Id is registered for alerts with the Bank
- Register complaint through multiple modes – as specified in point relating to Bank's roles & responsibilities
- Intimation at valid registered email/ mobile number with complaint number and date & time of complaint
- Receive compensation in line with this policy document wherever applicable. This would include getting shadow credit within 10 working days from reporting date and final credit within 90 days of reporting date subject to customer fulfilling obligations detailed herein and with customer liability being limited as specified in Annexure-I

B. Customer is bound by following obligations with respect to banking activities:

- Customer shall mandatorily register valid mobile number with the Bank.
- Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known email/ mobile number. Any failure of customer to update the Bank with changes shall be considered as customer negligence. Any unauthorized transaction arising out of this delay shall be treated as customer's liability.
- Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint and provide copy of the same to the Bank.
- Customer should co-operate with the Bank's investigating authorities and provide all assistance.
- 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 entity, including bank staff.
- Customer must protect his/her device as per best practices specified on the Bank's website, including updating of latest antivirus software on the device (Device includes smart phone,

THE K.C.C. BANK LTD. H.O. Dharamshala

feature phone, laptop, desktop, tab or any other devices used for accessing the banks electronic facilities.)

- Customer shall go through various instructions and awareness communication sent by the bank on secured banking available at banks website.
- Customer shall abide by the tips and safeguards on Secured Banking available at Bank's website.
- Customer must verify transaction details from time to time in his/her bank statement and raise query with the bank as soon as possible in case of any mismatch.

10. Notifying the Bank of the unauthorized transaction:

- Customer shall report unauthorized transaction to the Bank at the earliest, with basic details such as Account Number and/ or Card number (last 6 digits), date & time of transaction and amount of transaction
- Customer shall follow bank's reporting process viz.
  - Notify/ report through the options listed in the section on Roles & responsibilities of Bank (8 d).
  - Lodge police complaint and maintain copy of the same and furnish police complaint when sought by bank's authorized personnel.
- Customer shall authorize the bank to block the debit card/ net banking/ mobile banking / UPI / other channels of transaction in the account(s) to reduce likelihood of additional loss.
- Customer to clearly specify the facilities to be blocked failing which, the Bank reserves the right to block all electronic transactions of the customer to protect his/her interest.
- Customer shall share relevant documents as needed for investigation or insurance claim viz. cardholder dispute form, copy of passport in case of international transactions and police complaint.
- Fully co-operate and comply with Bank's reasonable requirements towards investigation and provide details of transaction, customer presence, etc.
- *For unauthorised transactions using KCCB Mobile App , customer shall block the disputed card in the KCCB mobile application or by mailing the details to KCCB on email id: dbdc@kccb.in*

11. Proof of customer liability:

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.

12. Redressal of Complaints / Grievance:

For any complaint / grievance with regard to services rendered by the Bank, customer has a right to approach authority (ies) designated by the Bank for handling customer complaint/ grievances.

They will be dealt in accordance with bank's Policy on Grievance Redressal. The details of the internal set up for redressal of complaints/ grievances will be displayed in the branch premises. The branch officials shall provide all required information regarding procedure for lodging the complaint. The same is also available in Bank's Website.

13. 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 "Acts 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 -1

Unauthorized Transaction due to Bank's negligence

Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	**Customer's Maximum Liability (Rs.)**
Customer to report as soon as possible to prevent future losses	Zero Liability
Unauthorized Transaction due to Customer's negligence	
Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	**Customer's Maximum Liability (Rs.)**
Customer to report as soon as possible to prevent future losses	100% liability till it is reported to Bank

Maximum Liability of a Customer in case of unauthorized Electronic Transaction where Responsibility is neither with the Bank nor with the customer but lies elsewhere in the system & customer has reported unauthorized transaction from transaction date within working days specified in following table:

Type of Account	**Within 3 working days (Rs.)**	**Within 4 to 7 working days (Rs.)**
PMJDY Accounts	Zero Liability	5000
All other SB accounts		10000
Current/ Cash Credit/ Overdraft Accounts of MSMEs		10000
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		10000
All other Current/ Cash Credit/ Overdraft Accounts		25000

***Any unauthorized electronic banking transaction reported after 7 working days will be treated as 100% customer liability.**

Format for Reporting Unauthorized Electronic Banking Transaction

To: The Branch Manager
Branch:.....

I	**Customer Information** Name of the customer : Account Number : Customer ID/CIF ID: Mobile Number : Email ID:
II	**Unauthorized Transaction Details :** Channel of transaction - Debit card/ Mobile Banking/Internet Banking/ UPI : Card Variant* - RUPAY Debit and Rupay KCC Card Type* - Domestic Total Amount Involved : Rs. Details of Unauthorized Transaction (mention all unauthorized transactions):
III	**Unauthorized Transaction Questionnair**
	1. How did you come to know about the disputed transactions? SMS□ Email □Account Statement □ Others (specify) □
	2. Have you received any calls/Email/SMS before the disputed transaction?Yes □No □
	3. If Yes, a) Phone Number/Email ID from which the request came: b) Have you shared any credentials like Card details, User ID, Password, ATM Pin, OTP, UPI Pin, Mpin, account details to the requester? Yes □ No □ c) Have you forwarded any SMS received? Yes □ No □ d) Have you clicked on any link received? Yes □ No □ e) Have you downloaded any app as instructed in the phone call/sms/email? Yes □ No □
	4. Status of the SIM card during the disputed transactions: Active □ Inactive□
	5. Were you in possession of your debit card at the time of unauthorized transaction?* Yes □ No □
	6. Have you surrendered the debit card at the Branch* Yes □ No □
	7. Mode of Reporting the Unauthorized transaction to Bank Customer Care □ Email □ Visit to Branch □ Others(specify) □
	8. Date & Time of reporting the Unauthorized transactions to Bank

DECLARATION

I hereby authorize the Bank to close the card, mobile banking and net banking immediately in my account due to Unauthorized transactions happened. I confirm that the averments made by me within this form are bona-fide and the information provided is true and accurate to the best of my knowledge and belief. In case this claim is determined by the Bank to be false or maliciously made, I shall be fully responsible for the consequences which may include civil/criminal lawsuit being initiated by the Bank. In case if bank compensates the loss due to the above mentioned disputed transactions either partly or fully, and if I/we receive any insurance claim subsequently for the same disputed transaction(s), I will inform the matter to the bank and agree to pay back the compensation paid by the bank.

Customer Name:_____ Signature: _____

(Seal is mandatory for business account holders)

Place:_____ Date:_____

*Mandatory if Unauthorized transaction happened via Debit Card

Note: Other fields are mandatory for all channels

Name & SS Code of the officer:

FOR OFFICE USE ONLY

Signature & Seal:

COMPLAINT DETAILS

Case Id :

Account number : **Received on :**

ACKNOWLEDGEMENT FROM BANK

RECEIVED BY

Name :

Designation & SSC: **Signature :**