The Jind Central Cooperative Bank Ltd., Jind

Policy for Customer liability

1. Introduction

The Jind Central Cooperative Bank Ltd is live on various alternate delivery channels. 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 and a policy was prepared. 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

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.

- Robust and dynamic fraud detection and prevention mechanism.
- Appropriate measures to mitigate risks and protect themselves against liabilities arising thereon.
- A system to educate customers in protecting themselves from frauds arising from electronic banking & payments.

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 etc.)

Customer Liability – 100% customer liability.

Customer Right – Customer to bear the entire loss until he / she reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne 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.

Loss due to negligence of a customer by sharing payment credentials will be borne by the customer till the time he reports the unauthorised transaction to the Bank. Loss occurring after reporting of unauthorised transaction to the Bank, shall be borne by the Bank.If the investigation establishes that the transaction is 2 factor authenticated liability of such transactions lies with customer, burden of proof lies with the bank

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 Bank's, Customer is having right to get compensation from Bank.

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.

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

Customer Liability – Based on the time taken by the customer to report the fraudulent transaction from the date of receiving the Bank communication as shown below.

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** of receiving the communication from the bank, Customer is having right to get compensation from Bank as per the details provided in the table below "**Summary of Customer's Liability"**

In such cases 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 (if any insurance was taken by the Bank) on best effort basis.

Customer Obligation – Customer is required to check the SMS / Email alert sent by Bank and approach the Bank as soon as the customer knows about unauthorized debit.

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	Basic Saving Bank Deposit accounts	Rs. 5000.00
	All other SB accounts, Pre-paid payment Instruments and Gift Cards, Current / Cash credit / Overdraft Account of MSMEs, Current Accounts / Cash Credit / Overdraft Account of Individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs. 25 lacs. Credit Card with limit upto Rs. 5 Lakhs.	Rs.10000.00
	All other Current / Cash Credit / Overdraft Account.	Rs. 25000.00

The number of working days mentioned in Table above shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

5. Aspects of Customer protection policy

Policy outlines the obligations on behalf of bank and customer to ensure the onus of liability arising out of fraudulent transaction.

Bank must ensure following:

- Appropriate systems and procedures to ensure safety and security of electronic banking transactions.
- Dealing quickly and empathetically with customer grievances.
- Mandatorily ask customers to register for SMS & wherever available register for E-mail alerts for electronic banking transactions.
- Mandatorily send SMS and wherever available send E-mail alerts for electronic banking transactions.
- Advise customers to notify unauthorised electronic banking transactions to Banks instantly upon occurrence.
- Facilitate reporting of unauthorised electronic banking transactions through Phone Banking, website(support section) IVR (dedicated helpline) and Branch network.
- Ensure immediate acknowledgement of fraud reported by customer.

- Take immediate steps on receipt of an unauthorised transaction from customer to prevent further damage.
- If the Bank identifies through external intelligence or during the course of its investigations, that the customer is a repeated offender in reporting fraudulent transactions, then it shall not only declare customer's liability, but also terminate the relationship with due notice .
- Bank will publish Do's and Don'ts for customers. 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.

Customer must ensure the following:

- Mandatorily register for SMS & Email alerts at the time of account opening.
- Mandatorily notify the Bank about any change of mobile number, email ID & communication address.
- Block/hotlist card or account if they suspect any malicious activities or in an event of lost /theft.
- Customers at any point should not disclose or share account details, credit card number, PIN , CVV with anyone over mail, calls or any other mode of communication.
- Confidentiality of password for internet banking & mobile banking should be ensured at all times.
- Customers to ensure passwords are kept secure and not to be recorded on paper or accessible electronic devices.
- Customer should check the transaction message triggered by bank and report any discrepancy immediately.
- Customer must submit necessary documentation to the bank as per defined timelines else the case stands closed under customer liability.
- Statement of account should be checked regularly and discrepancy if any should be reported to the Bank immediately.
- Passbook issued if any should be updated from time to time.
- Crossed / account payee cheques should be issued as far as possible.
- Blank cheques should not be signed and customers should not record their specimen signature either on pass book or cheque book.
- PIN & passwords should be changed on a regular basis
- Adher to "Do's and Don'ts" issued by the Bank

6. Resolution Time frame post reporting of fraudulent transaction

- 10 working days to provide temporary credit to customer from the date of reporting.
- Customer to submit necessary documentation within 30 days(20 days for Debit/RKC & Credit Cards) of reporting fraudulent transaction.
- Final resolution within 90 days

7. Channels to report fraudulent transactions by customers

- Phone Banking Channel
- Through support section at website (www.jinddccb.com)
- At Banks branches.
- Customers can report fraud via digital channels like Internet & mobile banking under the services & support section/Get support

8. Steps to be undertaken by Bank once customer reports fraud

- Bank to block the card (debit , credit or RKC card) on which the fraud is reported by customer.
- If fraud is reported through Internet or Mobile banking channels, Bank to de-register/de-activate the service to prevent any further mis-use.
- Bank to post temporary credit for the fraudulent transaction under consideration.
- Replace card plastic based on consent of customer.
- Restore/Activate Mobile, Internet banking facility & UPI based on customer consent.
- Advise customer on submission of fraud intimation along with the documents as mandated by the bank on the fraudulent transaction under consideration

9. Dispute Resolution Process (Standard Operating Procedure)

- 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.

iv) 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.

v) 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.

10. Burden of Proof

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

11. 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.