Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

---

Document Control

Document Name	**Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions**
Version	3.0
Document Owner	Chief Manager – Digital Products Department
Document Approver	Board of Directors
Effective from Date	From the date of Approval
Document Classification	Internal & External (For Customers using Digital Services of Bank)
Document Review Frequency	Once in two years or as per any changes in the Procedures, whichever is earlier
Document Applicable to	Digital Products Department (DPD) IT Department Other Product Offices and Regional Offices TJSB Branches Call Centre Support Staff Customers using TJSB's Electronic Banking Transactions

Document Revision History

Version	Document Date
1.0	15th Feb 2018
2.0	15th Feb 2020
3.0	27th Mar 2021

Ownership

This Document is owned by Chief Manager, Digital Products Department of TJSB Sahakari Bank Ltd. Unless, otherwise specified, no part of this document may be reproduced in any form, by any person. This document is for only Bank's Internal Usage and for Customers using Bank's Digital Services. The Policy shall be revised/ updated, whenever required/warranted by the owner of the policy.

Objective

To define a framework of rules, regulations, standards and practices to the Electronic Transactions initiated on / through TJSB Sahakari Bank Ltd.'s (also referred herewith as Bank, the Bank, TJSB, TJSB Bank) Electronic / Digital Products and to ensure that the same are in alignment with the best customer practices. TJSB Sahakari Bank Ltd. shall adopt adequate measures to safeguard and implement the defined guidelines in order to ensure that its Digital Products run on secured channel and in customer friendly manner.

For Customers of TJSB Sahakari Bank Ltd. only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

---

Validity and Review Frequency

Policy shall be valid for 2 year and reviewed / updated once in two years or in following scenarios,

- As and when required upon issue of guidelines from regulatory authorities,
- Launch of new feature/card product
- When there is change required in overall security of the product, business requirements or operational requirements.

Approval

The Policy and its revisions shall be placed by the Chief Manager of Digital Products Department to Executive Committee / Board of Directors once in two years. The Policy shall be approved by Executive Committee / Board of Directors.

Exemptions to the policy

- Exemptions to be sought from Managing Director and CEO and / or General Manager for any deviations to the Policy based on adequate business justification and recommendation / approval by respective Business Head / Region Head, unless otherwise specified in specific policy in this document.
- Managing Director and CEO and / or General Manager shall present such exemptions to Executive Committee or Board of Directors for approval / ratification.

Version Control

Chief Manager of Digital Products Department shall control the change and version of the policy document.

Distribution of Policy:

The Policy shall be distributed on Intranet, Banks Soft Board and on Banks official website for following departments/users;

- Digital Products Department (DPD),
- IT Department
- Other Product Offices and Regional Offices
- TJSB Branches
- Call Centre Support Staff
- Customers using TJSB's Electronic Banking Transactions

Policy Enforcement and Compliance

- Enforcement of the Policy shall be mandatory.
- Compliance with The Policy is mandatory for all applicants as per Applicability.

For Customers of TJSB Sahakari Bank Ltd.only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

---

INDEX

Background

TJSB Sahakari Bank Ltd., a Multi-State Scheduled Co-operative Bank registered under The Multi State Co-operative Societies Act 2002 and Rules made there under and having its Registered Office at TJSB House, Plot No.5 B, Road No.2, Wagle Industrial Estate, Thane West, 400604, Maharashtra, India, (hereinafter referred to as "Bank") puts best efforts to offer best customer service through offering range of Digital Products. Customer Service and Customers safety while initiating Electronic Banking Transactions are prime focus of Bank.

Policy Objectives

RBI vide its circular dated 14th December, 2017 no. DCBR.BPD.(PCB/RCB).Cir.No.06/ 12.05.001/2017-18 has issued guidelines on "Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions"

RBI has advised Co-operative Banks to implement their systems and procedures to make Customers feel safe while initiating electronic banking transactions. Banks are further advised to follow path as under,

- Create Robust and dynamic fraud detection and prevention mechanism.
- Building Mechanism for risk assessment to assess the risks resulting from unauthorized transactions and measure the liabilities arising out of such events.
- Measures to mitigate the risks
- Protection against the liabilities arising therefrom.
- Educating Customers to protect themselves against frauds arising out of Electronic Banking Transactions.

For Customers of TJSB Sahakari Bank Ltd.only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

---

Coverage of the policy

The Policy guidelines apply to Customers conducting electronic banking transactions using TJSB Products / Infrastructure such as, ATM/ Debit/ Prepaid/ Contactless Cards, ATMs / Cash Dispensers, Cash recyclers, Mobile Banking (Smart Money), Unified Payment Interface (TranZapp or any other UPI Apps), Bharat Bill Payment Service (BBPS), Internet Banking, QR-Code, etc. or other Bank's infrastructure such as ATM, POS, E-Com, UPI App etc.

The Policy covers the guidelines for determining the Customer's liability for unauthorized electronic banking transactions, its compensation. The Policy further covers aspects on creating customer awareness on the risks and responsibilities involved in electronic banking transactions on Remote / online transactions as well as face to face / physical transactions.

Validity

This Policy shall be reviewed once in two years in the light of changing scenarios and updation in RBI or any other Authorities' guidelines issued in this regards.

Bank Responsibilities/ Liabilities

- Install appropriate systems and procedures to ensure safety and security of electronic banking transactions.
- Attend to customer grievances.
- Making registration for SMS compulsory for electronic banking transaction to each customer
- Advise customers to notify unauthorised electronic banking transactions to Bank instantly upon occurrence.
- Facilitate reporting of unauthorised electronic banking transactions through Branch Banking, IVR at Customer Contact Centre (dedicated helpline) 24*7 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. Like Blocking of Card/s, Freezing of Internet Banking facility, Freezing of Mobile Banking Services, Freezing of A/c, etc.
- If the Bank identifies through external intelligence or during the course of its investigations, that the customer is a repeated complainant in reporting fraudulent transactions, then it shall not only declare customer's liability, but also terminate the relationship with due notice.

Customer Responsibilities / Liabilities

- Mandatorily register for SMS / Email facility at the time of account opening.
- Mandatorily notify the Bank about any change of mobile number, email ID & communication address.
- Immediately blocking of card or Account or Mobile App if they suspect any malicious activities or in an event of lost /theft of Card / Mobile.

For Customers of TJSB Sahakari Bank Ltd.only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

---

- Not to disclose or share account details, card number, PIN, CVV, MPIN, TPIN, UPI PIN or any type of passwords with anyone including spouse, son, daughter, friends, relatives, bank staff or any government employee at any given time, over mail, calls or any other mode of communication. Confidentiality of password is to be strictly maintained.
- Customers to ensure passwords are kept secure and not to be recorded on paper or accessible electronic devices.
- Customer shall not keep easily guessable password/s or any type of PIN/s. Customers to keep complex and non-guessable password/s.
- Any type of PINs & passwords shall be changed periodically on a regular basis by the Customer.
- Customer shall check the transaction message triggered by bank and report discrepancy, if any, immediately.
- Customer must submit necessary documentation to the bank as per defined timelines else the case stands closed under customer liability.
- Passbook issued if any shall be updated from time to time.
- Passbook / Statement of account shall be checked regularly and discrepancy if any shall be reported to the Bank immediately.
- Customer may install proper & authorised system securities (like antivirus) on his/her electronic devices such as Mobile, Laptop, Desktop, etc.
- Customer to ensure that application software shall be installed from official stores like Google Store, I-Store and after checking authenticity only.
- Customer shall ensure that, third party unauthorised software's, applications are not installed on his/her electronic devices like Mobile, Laptop, Desktop etc. which leads to Application frauds, Hacking, Skimming / cloning, account takeover, etc.
- In case of any queries, customer shall email to banks authorised email id (response@tjsb.co.in) and/or call to banks authorised helpline numbers (1800223466). Other authorised contact details of the Bank/Branch are available on banks website www.tjsbbank.co.in
- In case of card blocking, customer shall call to banks authorised helpline numbers (1800223466) or shall contact any of the TJSB Branch.

Burden of Proof of Customer Liability

- The burden of proving Customer liability in case of unauthorized electronic banking transactions shall be with the bank.
- Bank has implemented process of second factor authentication for electronic transactions, as regulated by the Reserve Bank of India. Therefore, Bank has onus to prove that all logs / proofs / reports for confirming two factor authentications are 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.

For Customers of TJSB Sahakari Bank Ltd. only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

- Bank may advise the Customer to file police complaint in case of unauthorised transactions. In such cases Customers shall fully co-operate with Bank and Police authorities or any enforcement authorities for filing compliant / FIR, disclosing all true & fair facts and without hiding any facts.
- During investigation, in case it is detected that the customer has falsely claimed or disputed valid transactions, the bank reserves its right to take due preventive action of the same including closing the account or limiting Electronic Transactions, etc.
- Bank may restrict customer from conducting electronic banking transaction including ATM transaction in case of non-availability of customer's mobile number.
- Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank shall 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 liability.
- Customer shall provide all necessary documentation as required by the bank to conduct the investigation, for determining customer liability for compensating the customer.
- Customer shall be co-operate with the Bank's investigating authorities and provide all assistance.

Insurance Cover

Bank shall cover its liability by taking adequate insurance cover either through its Banking indemnity policy, card protection policy or through cyber insurance policy wherever possible. Customer shall co-operate with Bank and/or Insurance Agency and/or Investigation Agency to provide FIR/Complaint copy registered with Police or any other documents as required in the case.

Defining Customer Liability

Banks Customer Protection for Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions is as under,

Liability burden	Brief Explanation	Case
(a) Zero Liability of the customer	The customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events,	(i) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).
		(ii) 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

For Customers of TJSB Sahakari Bank Ltd only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

		the bank within **three working days** of receiving the communication from the bank regarding the unauthorised transaction.
(b) Limited Liability of the Customer	The customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:	(i) In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, accepts or visits unauthenticated link forwarded by fraudulent person, the customer shall bear the entire loss until he/she reports the unauthorised transaction to the bank #. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.
		(ii) 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 the customer notifies the bank of such a transaction within **four to seven working days** of receiving a communication of the 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.
(c) Complete Liability of the Customer	The customer is fully liable for the loss occurring due to unauthorized transactions in the following cases:	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 Card PIN/ OTP or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing / Vishing attack, or any unauthenticated link. This could also be due to SIM deactivation by the fraudster. Under such situations, the customer shall bear the entire loss until the customer reports unauthorized transaction to 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 seven working days, the customer would be completely

For Customers of TJSB Sahakari Bank Ltd. only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

		liable for all such transactions.
		Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank shall 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 liability.

Bank has provided facility of Call Center which is available to Customer for blocking ATM/Debit Card 24 X 7 and for 365 days. In the event of any unauthorized transactions, Customer shall contact Call center no. 1800 223 466 and shall pass on account details or card number for blocking of Card to the Call Center executive. Alternatively, Customer can visit Branch and submit letter for blocking of Card. Bank shall provide acceptance on such letter alongwith Date and Time. As soon as the information for blocking the Card is received by Bank, (either by letter or on call center, and if the Card details which is to be blocked is clearly informed/ furnished/ mentioned then), Bank representative shall immediately block the card in the Customers' liability seizes and liability of any further transactions is transferred to Bank.

Table 1

Maximum Liability of a Customer under paragraph 2}

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	10,000
• All other Current/Cash Credit/Overdraft Accounts	25,000

Further, if the delay in reporting is beyond **seven working days**, the customer liability shall be determined. MD and CEO and / or General Manager are empowered to determine on case to case basis. Overall liability of the customer in third party breaches, as detailed in paragraph 1} and paragraph 2} above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised in the Table 2:

For Customers of TJSB Sahakari Bank Ltd.only

Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorised Electronic Banking Transactions

---

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	MD and CEO and / or General Manager are empowered to determine on case to case basis.

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.

Reversal Timeline for Zero Liability / Limited Liability of Customer

On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). The credit shall be value dated to be as of the date of the unauthorised transaction.

Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. In such cases, the detailed note for such a case would be put up before MD and CEO and / or General Manager for reimbursement to the Customer if any. Board / Executive Committee shall be informed about total number of cases periodically, also action taken thereon, the functioning of the grievance Redressal mechanism and take appropriate measures to improve the system and procedures.

However, in the case of failed electronic banking transactions, the terms of payment of customer compensation and TAT for such payment shall strictly be in accordance with provisions of RBI Cir. DPSS.CO.PD No.629/ 02.01.014/2019-20 dated September 20, 2019 on "Harmonization of Turn Around Time (TAT) and customer compensation for failed transactions using authorized Payment Systems" as laid down in the said circular.

In case of NFS ATM transaction, as per NPCI NFS OC – 317 dt.24th December 2018 EMV Liability Shift process, Bank is raising EMV Counterfeit Chargeback against acquirer bank and recover the loss amount. The TAT for Compliance or Acceptance of Chargeback from acquirer bank is 28 Calendar days. Hence, Bank shall wait for 28 days to give the clear credit in customer account.

---------- End of Document ----------

For Customers of TJSB Sahakari Bank Ltd. only