JIJAMATA MAHILA SAHAKARI BANK LTD,PUNE

Registered Office: Malati Madhav 1639 B, Sadashiv Peth , Tilak Road, Pune -411030

Customer Limiting Liability/Customer Protection & Awareness Policy

Version No 4.0

JIJAMATA MAHILA SAHAKARI BANK LTD. PUNE HEAD OFFICE

1. Overview

Jijamata Mahila Sahakari Bank Limited, Pune (hereafter referred to as "JMSB") has implemented RBI approved electronic banking channel products for the convenience of their customers. This policy of the Bank addresses customer's concerns and Reserve Bank of India's (hereafter referred to as "RBI") compliance requirement towards customer service for fraudulent transactions committed via Bank's electronic banking channel availed by respective customer. The Bank shall ensure that the policy is made available in domain (Bank's website & Branches).

2. Purpose

The purpose of the policy is to ensure that the systems and procedures in banks are designed to make customers feel safe and define customer liability while carrying out electronic banking transactions.Reserve Bank of India (RBI) has issued revised direction vide their Circular No. DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001/2017-18 Dated December 14, 2017.

3. Scope (Coverage of the policy)

This policy is applicable to fraudulent transactions via electronic banking channel products (offered by the Bank) in the Bank Accounts of all the customers of JMSB.

Electronic Banking Channels –

1. Automated Teller Machine (ATM) cum Debit Card Product
2. Mobile Banking including Immediate Payment System (IMPS)
3. Check Truncation System (CTS)
4. Unified Payment Interface (UPI)
5. Point Of Sale(POS)
6. E-Commerce Transaction(ECOM)
7. Electronic Clearing Service(ECS)

3.1 Automated Teller Machine (ATM) cum Debit Card Product

Bank is sub-member of HDFC Bank Limited for ATM cum Debit Card Product for National Financial Switch (NFS) membership of National Payments Corporation of India (NPCI). Bank is offering RuPay ATM cum Debit card product of NPCI. Bank has appointed M/s. Savatra Technologies Private Limited (Sarvatra) for processing ATM cum Debit Card Transactions. Sarvatra authenticates the card holder by PIN verification and does transaction routing between NPCI and the Bank, as required. Sarvatra is registered Application Service Provider (ASP) for ATM Switching and other product offerings of NPCI.

3.2 Mobile Banking Service

Bank has procured Mobile Banking application software of JJIT Fintech Private Limited to provide mobile banking service to the bank's customer having bank account at JMSB. This service is limited to savings, current bank account holder and staff cash credit account holders of the Bank. Bank has hosted the service side application of JJIT Fintech's mobile banking application software at the Bank's data center. Mobile Banking also covers Immediate Payment System (IMPS) services of NPCI. Bank is connected to NPCI through Sarvatra for IMPS service.

3.3 Check Truncation System (CTS)

Bank is sub member of HDFC BANK for Check Truncation System (CTS) system. Cheques are scanned in our Clearing Dept and uploaded on filezilla portal which is provided by HDFC bank to us.

3.4 Unified Payment Interface (UPI)

The Bank offers UPI services through Sarvatra Technologies. Customers can transfer funds instantly using Virtual Payment Address (VPA), mobile number, or QR code. UPI transactions are protected with two-factor authentication (device binding and MPIN), as per NPCI and RBI guidelines.

3.5 Point of Sale (POS)

POS terminals allow customers to pay at merchant establishments using RuPay debit cards. Transactions are authenticated through PIN or contactless methods within RBI limits. Customers must safeguard their cards, verify slips before signing, and promptly report unauthorized use.

3.6 E-Commerce Transactions (ECOM)

The Bank enables secure e-commerce payments using RuPay debit cards. Transactions are authenticated through One Time Passwords (OTP) under NPCI's 3D Secure framework. Customers must ensure merchant website genuineness and avoid sharing OTPs or card details.

3.7 Electronic Clearing Service (ECS)

JMSB provides ECS debit/credit services through HDFC Bank. ECS supports recurring transactions such as salary payments, EMI collections, and bulk debits/credits. Customers must regularly monitor account statements and report unauthorized ECS activity immediately.

4. Systems & Procedures:

Broadly, the Electronic Banking Transactions (EBT) is divided into two categories;

a) Remote / Online payment transactions / Card Not Present (CNP) Transactions where physical payment instruments are not required for making transactions for example; Mobile Banking.

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.)

5. Policy

i. At the time of account opening, bank is advising the customer to provide their mobile number to register for SMS alerts and email address to send transaction alert. This mobile number provided by the customer shall be registered mobile number entered in Core Banking Software (CBS). Bank shall send communication to the customer on this mobile number.

ii. Data Center in-charge shall ensure Bank's SMS alert delivery channel is operational. Accordingly Data Center in-charge shall monitor the availability of SMS package with the SMS delivery vendor. Data Center in-charge shall be responsible to recharge Bank's account with SMS delivery vendor, when number of balance SMS reaches 25,000.

iii. Bank is sending awareness message via SMS to registered mobile number to customers on at least 3 monthly basis.

iv. Data Center staff shall accept the customer complaint on mobile number and email (it@jijamatabank.com and **admin@jijamatabank.com Data**) Center staff shall be provided instructions to take a action immediately on the basis of customer complaint or contact Data Center In-charge / Senior Officer - IT Department immediately. This information shall be available on Bank's website (www.jijamatabank.com). Customers can also raise the complaint through the Bank's Official website i.e. www.jijamatabank.com.

v. To address customer complaint towards fraudulent electronic payment, Bank has set up a "Cyber Security Committee" On 25/09/2025. Following are be committee members -

   a. Chairman
   b. Director
   c. Chief Executive Officer

vi. This committee shall directly report to Board of Directors, if required. This committee shall be responsible for investigation of customer's claim towards fraudulent transaction. Committee shall refer to RBI's guidelines towards consumer protection. However, the decision to award the claim to customer as a gesture of goodwill rests with the Bank's Board of Directors.(Subject to valid reason for fraudulent transaction reported in time and validated after analysis.)

Customer Complaint procedure:

1. Any Branch can accept the written customer complaint within prescribed time limit. When Branch accept the compliant write time and date with officer sign and seal. After receiving the compliant Branch can report to the Nodal

Officer as early as possible and take necessary action. If Nodal officer is not available Branch can report to the CEO Immediately.

2. If any department of Head-Office can received customer complaint through E-mail or any other resources it will report to Nodal officer or CEO.

3. If IT department received any customer complaint, they will report to Nodal officer or CEO.

vii. Responsibility of Cyber Security Committee –

a. Review of IT infrastructure and Information Security related issues of the Bank. These issues may be highlighted by Bank's staff or auditors.
b. Plan of actions to -
   i. Address IT security risks of the Bank before implementation of Banking products
   ii. Comply with Reserve Bank of India's cyber security guidelines
c. Meeting frequency - quarterly basis

viii. On receipt of customer's complaint towards fraudulent transaction, Bank's representative shall contact the customer within 24 hours to provide information regarding further action initiated by the Bank. Bank shall also maintain record of this communication such as an email to registered email address / letter sent via Registered Acknowledgement Due (AD) mechanism / call recording.

ix. <u>Escalation matrix</u>

SN	Point of Contact	Designation	Level	Contact number	Email ID
1.	Jijamata Bank Helpline	Not applicable	1st	7774005243	it@jijamatabank.com
2.	Mr. Arun Manohar	Data Center In-Charge, Sr. Officer	2nd	8999112673	arunmanohar@jijamatabank.com
3.	Mr. Santosh Kulkarni	Deputy Chief Officer	3rd	9923732781	santoshkulkarni@jijamatabank.com
4	Mr. Preetam kumar Dedge	Nodal officer	4th	9881833710	preetamdedge@jijamatabank.com

5	Mr. Laxman Godambe	Chief Executive Officer	5th	9823411838	Laxmangodambe@jijamatabank.com

x. If Bank is unable to resolve aforementioned customer complaint or determine customer's liability within 90 days, the customer's account shall be credited with the amount of liability claimed on 90th day from the date of receipt of complaint.

xi. In case bank needs, Bank can escalate the issue to regulation/ court of laws. Bank may report the incident to respective regulatory authorities.

6. Guideline to customer for Safe Banking -

i. Change password and pin periodically.

ii. Don't share Debit Card details, OTP, PIN / passwords, CVV (printed at the back of the Debit Card) and User IDs with anyone.

iii. Don't record or write down the above information.

iv. Don't use easy to guess passwords / PIN (birthday, maiden name, date of birth, flat number, mobile number, etc.)

v. Do not allow others to use your Debit Card / credentials to use Bank's electronic payment channels such as mobile banking, etc.

vi. Immediately update the Bank in case of change of registered mobile number, email address and other details such as address registered with the Bank, etc.

vii. In case of loss of Debit Card / mobile phone with registered mobile application of the Bank or disclosure of PIN to others, immediately call the Bank on help number to disable the respective service.

viii. Verify the bank account statement on at least on monthly basis to ascertain the transactions in the bank account are legitimate. In case of identification of suspicious transactions, please contact the parent branch immediately or contact on helpline number (7774005243) or email address **admin@jijamatabank.com.**

ix. Use only EMV (chip) compliant cards of the Bank. Please contact your home branch of the Bank to avail free EMV card in exchange of old MagStrip (non-chip).

x. Ensure genuineness of merchant website before committing e-commerce transaction.Customer shall use the "Sarvatra Card Safe Application" available on Google Play Store in order to manage electronic transactions if not in use.

a. Customer shall allow/disallow ATM/POS/ECOM transactions.
b. Customer shall alter the transactional limit in Rupees of ATM / POS / ECOM.
c. Customer shall change the PIN periodically through the application to avoid the risk of fraud.

xii. In case of any emergency Customer can freeze account, using Bank is providing Miss call alert facility (for miss call alert number 9898367055)

7. Guideline for Bank for Cyber Security Controls

i. Conduct Information System Audit on annual basis covering –
   a. IT infrastructure
   b. Banking products
   c. Policies for IT Security Management/NPCI/CERT-IN
   d. Other applicable Reserve Bank of India guidelines

ii. Implement compliance for Information System Audit observations within 60 working days.

iii. Annual training to Board of Directors, Key Executives, IT Department and key banking operations Staff regarding implications of cyber security on Bank's services to customers.

iv. IT Infrastructure controls
   a. Anti-malware control on all computer systems of the Bank
   b. Implement firewall to allow only required network traffic
   c. Maintain CCTV cameras back up for ATMs at least 180 days and branch CCTV cameras back up for at least 180 days

V. Appropriate measures to mitigate the risks and protect themselves against the liabilities arising there-from;

a) Bank shall send alerts through mobile for all types of Card related and online banking transactions.

8. Risk Liability Matrix –

Sr. No.	Zero liability of the customer			
	Reason for fraudulent transaction	Customer compliant received since receipt of communication from Bank regarding fraudulent transaction	Liability on Customer / Bank	Amount
1.	Control failure of the Bank	Within 3 days	Bank	100% of Amount reported in fraudulent transaction
	Limited liability of the Customer as per RBI guidelines for consumer protection			
2.	Neither Bank nor customer but due to other entity in the payment system	4 to 7 days	For Customer Bank Account type 1.All other SB accounts 2 Current/Cash Credit/Overdraft Accounts of MSMEs 3 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)	Rs.10,000/-
			8.All other Current/Cash Credit/Overdraft Accounts	Rs.25,000/-
	Zero liability of the Bank			

3.	Customer negligence	Not applicable	Customer	100% of Amount reported in fraudulent transaction

i. Subscription to anti-phishing/ anti rogue ware system.
ii. SPF/DMARC control for email communication.
iii. Cyber insurance.

9. 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 written communication by the customer. The credit shall be value dated to be as of the date of the unauthorised transaction. The aforementioned credit (with shadow reversal) shall be valid till Bank concludes the investigation regarding complaint filed by the Customer. If Bank concludes not to award the claimed liability amount to the concerned Customer, the credited amount shall be immediately reversed by the Bank and accordingly inform to the Customer.

10. Customers' Responsibility

With respect to transaction using Jijamata Mahila Bank's Banking Channel, Bank shall not be responsible for loss, if any, incurred by the Customer due to Customer's negligence.

11. Record of Approval

	Prepared By :	Reviewed By :	Approved By :
Name	Mr. Santosh Kulkarni	Audit Committee	Board of Directors
Designation	Senior Officer, IT Department	-	-
Date	01/06/2020	23/06/2020	26/06/2020 Vide Resolution No.4
Update on	01/04/2022		30/04/2022 Res.No. 24
Review	29-09-2025		29-09-2025 Res. No. 3