Rajgurunagar Sahakari Bank Limited

Rajgurunagar, Dist. Pune.

Mobile Banking & UPI Policy

POLICY VERSION 1.8

REVISED UP TO MARCH 2026

Head Office
S.No319/320, Pune-Nashik Highway, Rajgurunagar
Taluka-Khed, Dist. Pune, Maharashtra - 410505

Mobile Banking & UPI Policy

This is a confidential document and is meant for restricted distribution.

Every person in custody of this document has the responsibility for ensuring its confidentiality. The custodian of the document will also ensure that the document is continually updated with amendments that may be issued from time to time. Any loss or mutilation of the document must be reported promptly to the next higher authority.

Board Resolution No. (3) Dated: 07/02/2018

Board Resolution No. (6) Dated: 28/02/2020

Board Resolution No. 5 (8)-1 Dated: 16/03/2022

Board Resolution No. 5 (12)-4 Dated: 28/03/2023

Board Resolution No. 5 (10) Dated: 26/03/2024

Board Resolution No. 4(12)-4 Dated: 10/03/2025

Board Resolution No. 5(19)-4 Dated: 24/03/2026

Mobile Banking & UPI Policy

Revision History

Date	Author	Version	Change Reference	Approval
25/02/2016	Rajgurunagar Bank	1.0	Document Created	Board Approval Dated 25/02/2016
07/02/2018	Rajgurunagar Bank	1.2	Document Modified	Board Approval Dated 07/02/2018
28/02/2020	Rajgurunagar Bank	1.3	Document Modified	Board Approval Dated 28/02/2020
14/03/2022	Rajgurunagar Bank	1.4	Document Modified	Board Approval Dated 16/03/2022
28/03/2023	Rajgurunagar Bank	1.5	Document Review	Board Approval Dated 28/03/2023
26/03/2024	Rajgurunagar Bank	1.6	Document Review	Board Approval Dated 26/03/2024
10/03/2025	Rajgurunagar Bank	1.7	Document Review	Board Approval Dated 10/03/2025
24-03-2026	Rajgurunagar Bank	1.8	Modified	Board Approval Dated 24/03/2026

Distribution List

Name	
Master copy	Chief Executive Officer
Controlled Copy	Asst. General Manager (IT Dept.)
Online Copy	For all employees of Rajgurunagar Bank

Mobile Banking & UPI Policy

Policy Statement

To strengthen transaction banking capabilities and deliver efficient, secure, and seamless digital services, the Bank shall provide a robust **Mobile Banking facility** to its customers.

The Bank is committed to offering **24x7 electronic banking services** through mobile platforms, ensuring convenience, security, and enhanced customer experience while adhering to applicable regulatory guidelines, including those issued by the Reserve Bank of India.

Objectives of Mobile Banking Policy

The objective of this policy is to establish a structured framework for the implementation, operation, and governance of the Bank's Mobile Banking Delivery Channel. The key objectives include:

- **24x7 Banking Service (Availability):**
  To provide customers with uninterrupted access to banking services anytime, anywhere through mobile devices.
- **Enhanced Customer Experience:**
  To improve customer convenience, satisfaction, and engagement by offering user-friendly and efficient digital services.
- **Competitive Positioning:**
  To strengthen the Bank's image, relevance, and competitiveness in the evolving digital banking ecosystem.
- **Customer Retention & Growth:**
  To increase customer loyalty and retention by delivering value-added digital banking services.
- **Operational Efficiency & Cost Optimization:**
  To reduce operational costs by encouraging migration from branch and ATM transactions to self-service digital channels.
- **Reduction in Physical Channel Load:**
  To decrease dependency on branch visits and ATM usage, leading to improved service efficiency.
- **Revenue Generation Opportunities:**
  To enable new revenue streams through digital payments, merchant services, and value-added offerings.
- **Security & Consumer Protection:**
  To ensure robust security controls, data protection, and compliance with regulatory requirements, safeguarding customer interests.

Mobile Banking & UPI Policy

Scope

This policy shall apply to the implementation, management, operation, and usage of the Bank's Mobile Banking Delivery Channel and shall cover the following:

- **Customers:**
  All customers of the Bank who are registered for and avail Mobile Banking services offered by the Bank.
- **Technology Infrastructure:**
  The complete IT infrastructure, applications, networks, security mechanisms, databases, and supporting systems associated with the Mobile Banking Delivery Channel at:
  - Kiya.ai (technology/service provider), and
  - Rajgurunagar Sahakari Bank Limited.
- **Bank Personnel:**
  Branch Managers, Officers, and Staff responsible for:
  - Customer onboarding and registration,
  - Customer awareness and digital literacy initiatives,
  - Grievance handling and support,
  - Operational monitoring and compliance related to Mobile Banking services.
- **Information Security & Compliance:**
  Security controls, authentication mechanisms, transaction monitoring, customer data protection, cyber security practices, and compliance with applicable regulatory and statutory guidelines issued by the Reserve Bank of India and other competent authorities.
- **Service Delivery & Support:**
  Processes relating to customer support, transaction processing, dispute resolution, incident management, business continuity, and service availability for Mobile Banking operations.

Channels to be used for Mobile Banking & UPI

a) Web App on Mobile
b) Unified Payment Interface (UPI)

Services to be offered through Mobile Banking & UPI

Functions available under Mobile Banking

i) Person to Person (P2P): This Enables the funds transfer from one account to another using Mobile Number and MMID – Mobile Money Identifier(In Process)
ii) Person to Account (P2A): This enables the funds transfer from one account to another using IFSC Code and Account Number)

iii) UPI based transaction.

Procedures for Mobile Banking Delivery Channel

Sr. No	Description
1.	**Ownership**
	a) The Head – Information Technology (IT) shall be the overall owner and custodian of the Bank's Mobile Banking Delivery Channel and shall be responsible for governance, oversight, security, regulatory compliance, and operational monitoring of the services offered to customers. b) The Mobile Banking application/platform may be developed, hosted, maintained, or supported by the Bank's authorized technology service provider, including Kiya.ai, while UPI-related services shall be operated through the infrastructure and systems of National Payments Corporation of India. However, the Bank shall retain overall responsibility and accountability for customer service, security, risk management, regulatory compliance, and protection of customer data. c) The Head – IT shall ensure that appropriate Service Level Agreements (SLAs), security clauses, confidentiality agreements, audit rights, and regulatory compliance requirements are incorporated in agreements executed with technology vendors and service providers. d) The Head – IT shall ensure that periodic Risk Assessments are carried out for the Mobile Banking ecosystem, including third-party integrations, APIs, UPI interfaces, and vendor-managed infrastructure, in accordance with the Bank's Information Security and Risk Management Policies. e) The Head – IT shall ensure implementation of adequate controls for: • Authentication and authorization, • Transaction security, • Monitoring and logging, • Fraud risk management, • Incident response, • Business continuity, and • Cyber security compliance. f) The Head – IT shall coordinate with the vendor, NPCI, auditors, and internal stakeholders for resolution of incidents, reconciliation issues, security events, customer grievances, and regulatory reporting requirements.

	g) The Head – IT shall ensure that periodic security audits, Vulnerability Assessment and Penetration Testing (VAPT), and compliance reviews of the Mobile Banking application and connected systems are conducted as per regulatory requirements issued by the Reserve Bank of India and applicable NPCI guidelines.
2.	**Customer Registration**
	a) Bank shall provide Mobile Banking services only to the customers who have applied to avail of this service and has completed KYC process. b) Bank shall devise and implement a legally acceptable Application Form for Customers detailing the security requirements, customer responsibility, and customer acceptance etc. before providing access to the Mobile Banking Delivery Channel. c) Mobile Banking Application form shall be made available at Branches of the Bank and shall also be made available on Google Play Store for Android Devices and Apple Store for IOS base Apple devices. d) Customers of the Bank shall take the Mobile Banking Application Form and duly filled in form shall be accepted at Branches and after signature, KYC and Account verification. e) After verification of the Account and KYC Compliance, Branches shall register the customer from the Mobile Banking Link provided to the Branches by LOGIN with their User Code and password and authorizing the registration in the system. f) After registration of the Form by Branches, Customers can download the Mobile Application of the Bank from Google Play Store for Android Phones shall activate the application after installation in the Mobile Phone. g) For registering the customer for the first time, Application will ask the Customer to enter 15 Digit Account Number and Registered Mobile Number and after authentication Application will ask for PAN number. After successful authentication Application will sent SMS for OTP and after entering OTP Customer can set MPIN for LOGIN and TPIN for transaction for funds transfer. h) Customers can download the Mobile Application from Google Play Store, Windows Store or Apple Store as per the device operating system. i) Frequently Asked Questions and Guidelines for using mobile banking shall be put on the web site of the Bank. j) Customer shall LOGIN to Mobile Application with MPIN given to the Customer and customer can do the functions as per the facilities defined in the Application k) For carrying out the Financial Transaction, customer shall use TPIN for every transaction for authentication. l) In case of Loss of Mobile Customer shall inform the Bank immediately so as to deactivate the Mobile channel.

	Device & Mobile Number Requirements • Mobile Banking and UPI services shall be available only on supported Android and iOS devices. • Customers shall use only non-rooted and non-jailbroken mobile devices for accessing the Bank's Mobile Banking and UPI services. • The mobile number registered with the Bank must be active and linked to the customer's device for OTP-based authentication and transaction alerts. • The Bank reserves the right to restrict or disable access from unsupported, compromised, rooted, jailbroken, or suspicious devices.
3.	Facilities Available for Customer under mobile Banking
	The following facilities/services shall be made available to customers through the Bank's Mobile Banking Application on Android and iOS platforms, subject to applicable regulatory guidelines, security controls, and transaction limits prescribed by the Bank from time to time: 3.1 Customer Registration & Authentication i. Customer registration through Debit/ATM Card authentication ii. MPIN and TPIN generation/change facility iii. Forgot/Reset PIN facility iv. De-registration of Mobile Banking services v. Two-Factor Authentication (2FA) for financial transactions 3.2 Account Information Services vi. Balance Inquiry vii. Mini Statement for recent transactions viii. Transaction search/history for 1 month, 3 months, and 6 months ix. View details of Deposits and Loan Accounts x. Manage Accounts including MMID and linked account information 3.3 Fund Transfer Services xi. Funds transfer between customer's own accounts xii. Internal funds transfer within the Bank xiii. Internal funds transfer to third-party accounts within the Bank xiv. Funds transfer through NEFT xv. IMPS Funds Transfer including Person-to-Account (P2A) and Person-to-Person (P2P) transactions

xvi. Beneficiary Account Name Lookup facility for IMPS and NEFT transactions
xvii. Beneficiary management and payee addition facility

3.4 Cheque & Card Related Services

xviii. Stop Cheque request facility
xix. Cheque Book request facility
xx. Debit/ATM Card hot-listing or hot card marking facility

3.5 Alerts & Customer Communication

xxi. SMS/notification alerts to customers upon successful completion of transactions
xxii. Bank contact information and customer support details
xxiii. Branch list and branch location details

3.6 Security & Control Features

xxiv. Transaction limit management for digital banking channels and contactless Debit/ATM Card services
xxv. Cooling period of 1 hour for activation of newly added beneficiaries/payees before permitting fund transfer transactions
xxvi. Security controls and authentication mechanisms as prescribed by the Bank and regulatory authorities

3.7 Future Enhancements

xxvii. Opening of Fixed Deposits through Mobile Banking and other digital banking services may be introduced in future based on business requirements, technical feasibility, and regulatory approvals.

The Bank may introduce additional services, features, and functionalities from time to time to improve customer convenience, operational efficiency, and digital banking experience, subject to compliance with guidelines issued by the Reserve Bank of India and National Payments Corporation of India.

4 Customer Eligibility shall be as per Table given below:-

Sr.	Type of A/c	Constitution	Mode of Op.	Who can operate
1	Savings A/c	Single	Single	The Account Holder
2	Savings A/c	Joint	Either or Survivor	Any One of the Accountholder authorized by both accountholders jointly. Application to be signed jointly.
3	Savings A/c	Joint	Jointly	Not Permissible
4	Savings A/c	Joint	Single	Not Permissible

5	Savings A/c	Student	Single	Minor above age of 14
6	Current A/C	Proprietor	Single	Accountholder
7	Current A/C	Partnership Firm	Any one partner	Any One of the Partner authorized by all the Partners as mentioned in the partnership deed. The application form for mobile banking shall be signed by all the Partners. Also obtain consent form duly signed by all partners.
8	Current A/C	Partnership Firm	Jointly Operated	Any One of the Partner authorized by all the Partners as mentioned in the partnership deed. Obtain indemnity bond from all partners regarding authorization of single partner. The application form for mobile banking shall be signed by all the Partners. Also obtain consent form duly signed by all partners.
9	Current A/C(LLP)	Partnership Firm	Jointly Operated	Any One of the Partner authorized by all the Partners as mentioned in the partnership deed. Obtain indemnity bond from all partners regarding authorization of single partner. The application form for mobile banking shall be signed by all the Partners. Also obtain consent form duly signed by all partners providing documents like LLP agreement, certificate of incorporation.

Ineligibility Conditions:

The following customers shall not be eligible for activation or continued usage of Mobile Banking/UPI facilities:

- Accounts classified as dormant or inoperative for a continuous period exceeding twelve (12) months, unless reactivated as per Bank policy.
- Customers subject to fraud monitoring, internal blacklist, caution list, regulatory restrictions, or law enforcement lookout notices.
- Customers whose KYC is incomplete, expired, or non-compliant.
- Customers identified as high-risk based on fraud monitoring or suspicious transaction patterns.
- Customers prohibited under applicable RBI, NPCI, FIU-IND, or statutory guidelines.
- Customers identified under sanction lists, mule account monitoring, or fraud risk databases may be restricted from availing Mobile Banking/UPI services.

5	**Technology& Security Standards to be adopted for Mobile Banking**
	The Bank shall adopt appropriate technology, cyber security, and risk management controls for the Mobile Banking Delivery Channel to ensure confidentiality, integrity, availability, authentication, and protection of customer information and transactions. 5.1 Platform & Application Security a) The Bank shall provide Mobile Banking Application services on Android and iOS platforms. b) Customers shall be able to download and install the Mobile Banking Application after successful registration with the Bank. During activation, One Time Password (OTP) authentication shall be carried out on the customer's registered mobile number. Customer identity verification may include validation of PAN or other officially valid documents (OVD), as applicable. c) Customers shall be required to set MPIN and TPIN credentials during activation of Mobile Banking services: • MPIN shall be mandatory for login and non-financial transactions. • TPIN shall be mandatory for financial transactions and transaction authentication. d) MPIN and TPIN credentials shall not be stored in plain text on the customer's mobile device. e) Customers shall be allowed a maximum of three consecutive incorrect login attempts using MPIN/User ID. Upon exceeding the permitted attempts, the Mobile Banking access shall be temporarily locked as per the Bank's security policy. f) MPIN shall have a validity period of 365 days, after which customers shall be required to change/reset the MPIN. g) Mobile Banking registration and activation shall be linked with the customer's registered mobile number maintained in the Bank's records. h) Two-Factor Authentication (2FA) shall be implemented for customer authentication and validation of the registered mobile number in compliance with applicable regulatory guidelines.

5.2 Transaction Authentication & Encryption

i) All sensitive information including MPIN, TPIN, authentication credentials, and transaction data transmitted between the customer device and server shall be encrypted using secure communication protocols and industry-standard cryptographic controls.

j) MPIN generation and cryptographic key management shall be implemented using secure mechanisms such as Hardware Security Module (HSM) or equivalent secure infrastructure.

k) Encryption and decryption controls shall be implemented for all requests and responses exchanged through the Mobile Banking system using secure SSL/TLS-based communication channels and other security standards prescribed by the Bank and regulators.

l) Transaction limits for Mobile Banking services shall be implemented in accordance with guidelines issued by the Reserve Bank of India and applicable payment system regulations.

5.3 Beneficiary & Transaction Controls

m) Addition of new beneficiaries/payees shall be subject to a cooling period of 60 minutes or such period as prescribed by the Bank/regulator from time to time. Financial transactions to newly added beneficiaries shall be permitted only after expiry of the cooling period.

n) SMS and/or email alerts shall be sent to customers for:

- Beneficiary addition/deletion,
- Financial transactions,
- Profile modifications, and
- Other critical account activities.

o) Session timeout controls shall be implemented. The Mobile Banking application shall automatically disconnect/logout after 120 seconds of inactivity or as per security policy defined by the Bank.

p) Any change in customer profile details, including mobile number modification, shall be carried out only after proper customer identification, due verification, and compliance with KYC requirements at the customer’s home branch or through approved secured processes.

5.4 Monitoring, Logging & Fraud Prevention

q) Logs of all Mobile Banking operations, activities, and transactions shall be maintained and preserved for monitoring, audit trail, reconciliation, incident investigation, and fraud detection purposes as per regulatory and internal policy requirements.

r) The Bank shall implement adequate fraud risk management and transaction monitoring mechanisms for identifying suspicious, unusual, or unauthorized activities.

5.5 Infrastructure & Network Security

s) The Mobile Banking system shall be deployed using secure multi-tier architecture including Demilitarized Zone (DMZ), firewalls, intrusion detection/prevention systems, and other network security controls.

t) Appropriate physical and logical security controls shall be implemented to protect servers, databases, gateways, network equipment, applications, and supporting infrastructure from unauthorized access, tampering, malware, cyber-attacks, and environmental threats.

u) The Bank and its service providers, including Kiya.ai, shall ensure adequate wired and wireless network security protection mechanisms at Data Centre (DC) and Disaster Recovery (DR) sites.

5.6 Security Assessment & Compliance

v) The Bank and/or PSP application may implement SIM binding, device fingerprinting, and device integrity verification controls for fraud prevention and secure customer authentication.

w) Periodic Risk Assessment, Vulnerability Assessment and Penetration Testing (VAPT), application security review, cyber security audit, and network security assessment of the Mobile Banking environment shall be conducted at least annually or at such intervals as prescribed by regulators.

x) The compliance status of security observations and audit findings shall be monitored by the Bank and significant observations shall be placed before the Board / IT Strategy Committee / Information Security Committee, as applicable.

z) The Mobile Banking Delivery Channel shall comply with applicable guidelines and directions issued by the Reserve Bank of India, National Payments Corporation of India, and other relevant statutory or regulatory authorities.

6	**Responsibilities of the Customer**
	The customer availing Mobile Banking and UPI services shall comply with the following responsibilities and obligations: 6.1 Responsibility for Transactions The customer shall be responsible for all transactions carried out through the registered mobile device, SIM card, Mobile Banking credentials, UPI credentials, MPIN, TPIN, OTP, debit card credentials, or any other authentication mechanism, whether authorized or unauthorized, until such loss, theft, misuse, or compromise is reported to the Bank through prescribed channels. Any transaction authenticated using valid credentials shall be deemed to have been initiated by the customer unless reported otherwise to the Bank within the prescribed timelines. 6.2 Safeguarding of Credentials The customer shall be solely responsible for maintaining confidentiality and secrecy of: • UPI PIN, • MPIN, • TPIN, • OTPs, • Device password/PIN, • Debit Card credentials, and • Any other authentication credentials. The customer shall: • Keep all credentials confidential and secure, • Use Mobile Banking services strictly in accordance with procedures prescribed by the Bank, • Immediately change credentials upon suspicion of compromise. The customer shall not: • Write down or store credentials in an insecure manner or on the mobile device, • Share credentials with any person, • Disclose OTPs or PINs to anyone including persons claiming to represent the Bank, Reserve Bank of India, National Payments Corporation of India, telecom operators, police authorities, or service providers, • Disclose credentials through phone calls, SMS, email, social media, remote access applications, or any electronic medium.

The Bank shall never ask customers for UPI PIN, OTP, MPIN, TPIN, or Debit Card PIN through phone calls, SMS, email, or social media.

6.3 Device and Application Security

The customer shall:

- Use only non-rooted/non-jailbroken mobile devices,
- Install applications only from official app stores,
- Maintain updated operating systems and security patches,
- Install and maintain appropriate anti-malware/security software wherever applicable,
- Avoid use of public or unsecured Wi-Fi networks for financial transactions,
- Ensure physical security of the mobile device and SIM card,
- Promptly review transaction alerts and account statements.

The customer shall not:

- Install applications from untrusted or unknown sources,
- Permit screen-sharing or remote-access applications during banking activity,
- Store screenshots/images containing sensitive banking information.

6.4 Reporting of Unauthorized Transactions

The customer shall immediately report:

- Unauthorized transactions,
- Loss or theft of mobile handset,
- SIM card loss/cloning,
- Compromise of credentials,
- Suspicious/fraudulent activity,
- Unauthorized access to Mobile Banking services.

In case of loss, theft, compromise, or unauthorized access to the mobile device or SIM card, the customer shall immediately:

- Contact the Bank’s helpline/branch and request blocking of Mobile Banking/UPI services,
- Block the SIM card through the telecom service provider,
- file police complaint/FIR wherever required and provide copy to the Bank, if requested.

The customer shall report unauthorized electronic banking transactions immediately upon receipt of SMS/email alert and preferably within three (3) working days to avail protection under applicable RBI guidelines on customer liability for unauthorized electronic banking transactions.

Delay in reporting may increase customer liability in accordance with applicable regulatory guidelines and Bank policy.

6.5 Verification of Beneficiary Details

The customer shall verify beneficiary details, including beneficiary name displayed through account verification/name lookup facility, before authorizing any transaction.

The Bank shall not be liable for incorrect transfers arising due to:

- Incorrect beneficiary details entered by the customer,
- Failure of the customer to verify beneficiary name/details,
- Mistaken transfers to unintended beneficiaries.

6.6 Prohibited Usage

The customer shall not use Mobile Banking or UPI services for:

- Unlawful or fraudulent transactions,
- Money laundering activities,
- Gambling or betting activities,
- Transactions prohibited under applicable laws,
- Activities prohibited by the Reserve Bank of India, National Payments Corporation of India, FIU-IND, or any statutory authority,
- Transactions violating the Bank’s acceptable use or security policies.

The Bank reserves the right to decline, suspend, reverse, freeze, or report such transactions to regulatory or law enforcement authorities wherever required.

6.7 Liability of Customer

Any financial loss arising due to:

- Disclosure or sharing of credentials by the customer,
- Negligence in safeguarding device or credentials,
- Use of rooted/jailbroken or malware-infected devices,
- Delay in reporting unauthorized transactions,
- Breach of obligations under this policy,
- Failure to follow security advisories issued by the Bank,

shall be borne by the customer to the extent permissible under applicable laws, regulatory guidelines, and Bank policy.

	6.8 Awareness of Bank Communications The customer shall keep himself/herself updated regarding: • Terms and conditions, • Security advisories, • Changes in services, • Transaction limits, • Operating procedures, • Regulatory updates, Published by the Bank through its website, Mobile Banking application, branches, SMS/email alerts, or other official communication channels.
7	**Interoperability**
	The Bank shall provide interoperability for Mobile Banking and digital payment services through payment systems and infrastructure operated by National Payments Corporation of India, including: • Unified Payments Interface (UPI), • Immediate Payment Service (IMPS), • Other NPCI-enabled interbank payment systems introduced from time to time. Through such interoperable payment systems, customers shall be able to perform interbank fund transfer transactions with participating member banks subject to: • Applicable regulatory guidelines, • NPCI operating rules, • Transaction limits, • Security controls, • Bank's internal policies. The Bank shall ensure that interoperability services are implemented in compliance with guidelines issued by the Reserve Bank of India and NPCI, including requirements relating to authentication, transaction security, dispute resolution, reconciliation, fraud risk management, and customer protection.
8	**Clearing and Settlement for Interbank funds Transfer Transaction**
	The Bank is a direct member of the Mobile Banking payment systems operated by National Payments Corporation of India for: • Immediate Payment Service (IMPS), and • Unified Payments Interface (UPI).

	Accordingly, interbank fund transfer transactions initiated through Mobile Banking shall be processed through the NPCI network and payment infrastructure. All interbank settlements relating to IMPS, UPI, and other NPCI-enabled payment systems shall be carried out by NPCI through settlement mechanisms approved by the Reserve Bank of India, including debit and credit to the Bank's designated RTGS/current settlement account maintained for such purpose. The Bank shall comply with all operational, settlement, reconciliation, security, dispute management, and risk management guidelines prescribed by NPCI and RBI from time to time.
9	**Transaction Limits on Mobile Banking**

The Bank shall prescribe transaction limits for Mobile Banking transactions in accordance with guidelines issued by the Reserve Bank of India, National Payments Corporation of India, internal risk management framework, and customer risk profile.

9.1 IMPS and NEFT Transaction Limits

a) The following transaction limits shall apply for transactions performed through the Mobile Banking Application using encrypted authentication mechanisms:

Transaction Type	Per Transaction Limit	Daily Aggregate Limit
IMPS	₹5,00,000/-	₹5,00,000/-
NEFT	₹5,00,000/-	₹5,00,000/-
Overall Combined Daily Limit	—	₹10,00,000/-

b) Based on customer request and recommendation of the concerned Branch Manager, the overall daily transaction limit may be enhanced up to ₹15,00,000/- per day, subject to:

- Satisfactory account conduct,
- Valid KYC compliance,
- Customer risk assessment,
- Execution of required undertaking/documents, and
- Approval by competent authority.

The enhanced limits may be structured as follows:

Transaction Type	Enhanced Daily Limit
IMPS	₹5,00,000/-
NEFT	₹10,00,000/-

Overall Combined Daily Limit	₹15,00,000/-

c) Any request for NEFT transaction limit enhancement beyond ₹10,00,000/- through Mobile Banking shall require:

- Written request from the customer,
- Recommendation of the concerned Branch Manager, and
- Approval from the Bank's IT Committee or other competent authority designated by the Bank.

The transaction limit shall be revised only after formal approval by the competent authority.

9.2 UPI Transaction Limits

a) The standard transaction limit for transactions performed through Unified Payments Interface (UPI) shall be:

Transaction Type	Per Transaction Limit	Daily Aggregate Limit
UPI	₹50,000/-	₹1,00,000/-

b) As per NPCI Circular OC-185 dated 19 December 2023 and RBI Statement on Developmental and Regulatory Policies dated 08 December 2023, the per transaction limit for UPI transactions may be enhanced up to ₹5,00,000/- for specific merchant categories including:

- Hospitals/Healthcare Services, and
- Educational Institutions/Services,

subject to:

- Merchant category eligibility defined by NPCI,
- Merchant verification by NPCI/acquiring institution,
- Applicable regulatory guidelines and system controls.

c) Customers requiring transaction limits higher than the standard limits prescribed by the Bank shall submit a written application to the branch for enhancement within the maximum permissible limits approved by the Bank.

Such requests shall be processed subject to:

- Completion and validity of KYC,
- Satisfactory operation in the account,
- Customer risk profile and due diligence,

	• Execution of risk undertaking/indemnity wherever applicable, • Approval by competent authority as per Bank policy. 9.3 General Conditions a) The Bank reserves the right to: • Revise transaction limits, • Impose additional restrictions, • Decline transactions, • Temporarily suspend transaction facilities, based on risk perception, regulatory instructions, fraud monitoring, suspicious transaction patterns, system security requirements, or operational considerations. b) All transaction limits shall be subject to: • Applicable RBI and NPCI guidelines, • Fraud risk management controls, • System capabilities, • Customer authentication requirements, • Internal security policies of the Bank. c) The Bank may prescribe separate limits for: • Financial and non-financial transactions, • Newly added beneficiaries, • Contactless transactions, • Merchant payments, • High-risk transactions/categories, • First-time users or newly activated accounts.
10	**Modification in Application**
	a) The Bank shall have the absolute right and discretion to: • Modify, upgrade, suspend, discontinue, or supplement any feature, functionality, service, facility, or benefit offered under the Mobile Banking platform, • Introduce new services or revise existing services • Change transaction limits, operating procedures, security requirements, or eligibility criteria, based on business, operational, security, technological, or regulatory requirements.

	b) The Bank may also modify the Mobile Banking Application, user interface, authentication mechanisms, transaction workflows, or security controls from time to time to comply with technological advancements, cyber security requirements, and regulatory guidelines issued by the Reserve Bank of India, National Payments Corporation of India, or other statutory authorities. c) The Bank shall communicate the Terms and Conditions governing Mobile Banking services and any amendments thereto through: • The Bank's official website, • Mobile Banking application, • SMS/email notifications, • Branch notices or any other communication channel considered appropriate by the Bank. d) Customers shall be responsible for regularly reviewing the updated Terms and Conditions, security advisories, transaction limits, and operational instructions published by the Bank. e) Continued use of the Mobile Banking Facility after publication/communication of amendments shall constitute deemed acceptance of the revised Terms and Conditions by the customer. f) The Bank reserves the right to temporarily suspend or restrict access to Mobile Banking services for maintenance activities, system upgrades, security concerns, regulatory compliance, fraud prevention, or operational exigencies without prior notice wherever necessary.
11	**Unified Payment Interface System**
	The Bank shall offer Unified Payments Interface (UPI) services to its customers under the issuer bank model through the payment infrastructure operated by National Payments Corporation of India. 11.1 UPI Framework a) UPI enables customers to perform interoperable digital payment transactions using Virtual Payment Address (VPA), account number with IFSC, mobile number, QR code, or other identifiers permitted under the UPI ecosystem. b) UPI provides customers with an email-like Virtual Payment Address (VPA) for facilitating secure transactions without sharing bank account details. Customers may create multiple VPAs as permitted under NPCI guidelines and supported PSP applications.

c) To protect customer privacy, account mapping information shall remain within the banking system and shall be managed in accordance with applicable security and privacy standards.

d) The Bank shall act as issuer bank and customer registration for UPI services may be enabled through third-party PSP/TPAP applications used by customers, subject to authentication through Debit/ATM Card credentials, UPI PIN, OTP, device binding, and other regulatory authentication requirements.

e) Customers may download NPCI-approved UPI-enabled PSP applications from official app stores and link their Bank accounts for availing UPI services.

11.2 Eligibility and Registration

a) UPI services shall be available to customers maintaining satisfactorily conducted Savings or Current Accounts in individual capacity with the Bank.

b) The customer must:

- Have a mobile number registered with the Bank,
- Ensure that the same mobile number is linked with the bank account and Debit/ATM Card,
- Comply with eligibility conditions prescribed by the Bank, NPCI, and RBI.

c) Customer registration for UPI services may be completed through authorized PSP applications using Debit/ATM Card authentication, OTP validation, and UPI PIN creation.

d) As per NPCI guidelines, TPAP/PSP applications may suspend or deactivate customers who have not performed any financial or non-financial UPI transaction for a continuous period of one year.

11.3 UPI Transaction Limits and Security

a) Standard UPI transaction limits shall be applicable as prescribed by the Bank, NPCI, and RBI from time to time.

b) Entering incorrect login password or authentication credentials repeatedly may result in temporary blocking of the application/account in accordance with security controls implemented by the PSP application or the Bank.

c) Customers shall use only their own registered mobile number/device for accessing UPI applications and services. Access shall be restricted to the mobile number registered with the Bank for UPI services.

d) Customers are advised to:

- Maintain sufficient account balance before initiating transactions,
- Enter correct UPI PIN and credentials,
- Avoid repeated failed transaction attempts,
- Follow cyber security precautions issued by the Bank and NPCI.

11.4 Customer Responsibilities and Liability

a) The customer shall be responsible for all transactions initiated using the registered UPI application and credentials.

b) The customer shall immediately inform the Bank and the concerned PSP application provider in case:

- Mobile number is changed, lost, or allotted to another person,
- Unauthorized access or suspicious transaction is noticed,
- UPI credentials are compromised.

c) The customer shall ensure deregistration/blocking of UPI services through the PSP application and/or Bank wherever required.

d) Dispute resolution relating to UPI transactions shall be governed by NPCI guidelines and applicable regulatory framework issued from time to time.

11.5 Liability of the Bank

a) The Bank shall not be liable for non-availability, interruption, or delay in UPI services arising due to:

- Natural calamities,
- Floods, fire, or other disasters,
- Telecommunication/Network failure,
- System failure of PSP/TPAP/NPCI,
- Legal restraints or reasons beyond the control of the Bank.

b) The Bank shall not be responsible for:

- Issues arising out of third-party PSP/TPAP applications,
- Incorrect beneficiary details entered by the customer,
- Wrong credits/transfers due to customer error,
- Interruption of business, indirect loss, consequential damages, or loss of goodwill/profit.

	c) The customer expressly authorizes the Bank to access, process, and share account information with NPCI, PSPs, TPAPs, regulators, or authorized third parties as required for providing UPI services and complying with legal/regulatory obligations. d) Transaction records maintained by the Bank shall be treated as conclusive proof of authenticity and accuracy of transactions, subject to applicable laws and dispute resolution mechanisms. The Bank may preserve such records for the period prescribed under applicable laws and regulatory requirements. e) The Bank shall make reasonable efforts to maintain confidentiality and security of customer information; however, the Bank shall not be liable for disclosure of information caused by reasons beyond its control or due to actions of third parties. **11.6 Liability Exclusions** The Bank shall not be liable for losses arising from: • Unauthorized access to the customer's mobile device due to theft, hacking, compromise, or negligence, • Voluntary disclosure of UPI PIN, OTP, MPIN, TPIN, card credentials, device credentials • Usage of rooted, jailbroken, compromised, or malware-infected devices, • Incorrect beneficiary details entered by the customer, • Telecom network failure or internet connectivity issues beyond the Bank's control, • Force majeure events including natural disasters, cyber incidents affecting external infrastructure, NPCI outages, power failures, strikes, or regulatory restrictions.
	Dispute Management in UPI
	a) Definition of Failed Transaction A "Failed Transaction" means a transaction that has not been fully or successfully completed due to reasons not attributable to the customer, including but not limited to: • Communication or network failure • Technical failure in banking/payment systems • Session timeout • Non-availability of services • Delayed response from participating systems • Beneficiary account validation failure • Incomplete or incorrect transaction processing • Delayed or non-initiation of reversal transactions Failed transactions shall also include cases where: • Customer account is debited but beneficiary account is not credited

	• Transaction status remains pending • Credit could not be effected due to incomplete or incorrect beneficiary information • Reversal of failed transactions is delayed beyond prescribed timelines. b) Reporting of Complaints by Customers a) Customers shall report failed or disputed transactions within the timelines prescribed by National Payments Corporation of India and the Reserve Bank of India from the date of transaction. b) Complaints may be reported through: • Branch, • Bank grievance portal • NPCI Complaint Portal • Any other approved channel made available by the Bank. • PSP Application c) Customers shall provide relevant transaction details including: • Transaction date, • Transaction amount, • Transaction reference number (RRN/UTR), • Beneficiary details, • Merchant details/slip in case of merchant transactions, • Screenshots or supporting records wherever applicable. c) Handling of Delayed Complaints a) If a customer reports a failed electronic transaction beyond the timelines prescribed under applicable NPCI/RBI guidelines, the complaint may be registered by the Bank on a "good faith" basis. b) In such cases: • Compensation may not be payable, • Resolution shall depend upon recovery/settlement from participating banks or payment system operators. c) Turn Around Time (TAT) for good faith chargeback/dispute handling shall be governed by applicable NPCI/RBI guidelines and card/payment network rules prevailing from time to time.

d) Chargeback and Dispute Processing

a) The Bank, acting as remitter bank, shall initiate chargeback/dispute requests through NPCI systems/portal within prescribed timelines.

b) Complaints received up to 4:00 PM on a working day shall ordinarily be processed on the same day.

c) Complaints received after 4:00 PM or on holidays/non-working days shall ordinarily be processed on the next working day.

d) All disputes shall be handled in accordance with:

- NPCI operating and procedural guidelines,
- RBI directions,
- Internal dispute resolution procedures of the Bank.

e) Interbank Dispute Handling

a) Where a customer initiates UPI/IMPS/NEFT transaction from another bank (remitter bank) to an account maintained with Rajgurunagar Sahakari Bank Limited and the remitter account is debited without credit to the beneficiary account, the customer shall approach the respective remitter bank for lodging the complaint.

b) The remitter bank shall act as the primary point of contact for dispute resolution in such cases in accordance with NPCI/RBI guidelines.

f) Time Frame for Resolution

The Bank shall endeavor to resolve failed transaction complaints within the following indicative timelines or such timelines as prescribed by RBI/NPCI from time to time:

Transaction Type	Resolution Timeline
UPI Person-to-Person / Fund Transfer	T + 1 Calendar Day
UPI Merchant Transactions	T + 1 Calendar Day
IMPS Fund Transfer Transactions	T + 1 Calendar Day

(T = Date of Transaction)

g) Customer Compensation

	a) If failed transaction disputes are not resolved within the timelines prescribed by applicable RBI/NPCI guidelines, compensation shall be payable to the customer in accordance with: • RBI circulars/directives, • NPCI dispute management guidelines, • Bank's Customer Compensation Policy. b) Compensation shall not be payable in cases where delay occurs due to: • Incorrect information provided by the customer, • Customer negligence, • Force majeure events, • System failure beyond the control of the Bank, • Delayed complaint reporting beyond prescribed timelines. h) Record Maintenance and Monitoring The Bank shall maintain proper records of: • Disputed transactions, • Chargeback requests, • Reversals, • Customer complaints, • Compensation paid, • Unresolved disputes, for audit, monitoring, reconciliation, fraud risk management, and regulatory reporting purposes.
12	**Risk Mitigation Measures to be adopted by the Bank**
	The Bank shall implement appropriate technical, operational, administrative, and security controls to mitigate risks associated with Mobile Banking and digital payment services. 12.1 Application and Data Security a) The Mobile Banking Application shall not store sensitive financial information, authentication credentials, or confidential account-related data in plain text on the customer's mobile device. b) All customer data, transaction information, authentication credentials, and communication between the Mobile Banking Application and Bank systems shall be

encrypted using secure cryptographic protocols and industry-standard security mechanisms.

c) Secure session management, device binding, timeout controls, encryption, and authentication mechanisms shall be implemented to prevent unauthorized access and misuse.

13.2 Authentication and Access Control

a) Two-Factor Authentication (2FA) shall be implemented for financial transactions in accordance with guidelines issued by the Reserve Bank of India and National Payments Corporation of India.

b) Transaction Password (TPIN), UPI PIN, OTP, or other approved authentication mechanisms shall be used as additional authentication factors for validating financial transactions.

c) Login attempt restrictions, session timeout controls, password expiry controls, and customer/device verification mechanisms shall be implemented to reduce unauthorized access risks.

12.3 Customer Awareness and Education

a) The Bank shall conduct customer awareness and cyber security education programs relating to safe usage of Mobile Banking services.

b) Customers shall be advised:

- Not to share mobile devices, MPIN, TPIN, OTP, UPI PIN, or Debit Card credentials with any person,
- Not to hand over mobile phones to unknown persons or third parties for banking transactions,
- Not to disclose credentials over phone calls, SMS, email, social media, or remote access applications
- Install applications only from authorized app stores,
- Avoid fraudulent links, phishing attacks, QR code scams, and social engineering attempts.

c) The Bank may periodically issue security advisories through SMS, email, website notifications, branch notices, and Mobile Banking application alerts.

12.4 Transaction Monitoring and Fraud Risk Management

a) The Bank shall implement transaction monitoring mechanisms for identifying suspicious, unusual, fraudulent, or high-risk transactions.

b) The Bank shall monitor movement of funds through Mobile Banking channels and may:

- Decline transactions,
- Block/suspend accounts or services,
- Impose restrictions,
- Seek additional customer verification,

where suspicious or fraudulent activity is detected.

c) Logs and audit trails of Mobile Banking transactions and activities shall be maintained for fraud detection, investigation, reconciliation, audit, and regulatory reporting purposes.

12.5 Transaction Limits and Control Measures

a) Transaction limits shall be implemented for Mobile Banking services to reduce fraud and operational risk exposure.

b) The standard aggregate daily transaction limit for Mobile Banking transactions shall ordinarily be ₹10,00,000/- per customer or such revised limits as prescribed by the Bank from time to time.

c) Additional controls such as:

- Cooling period for newly added beneficiaries,
- Transaction velocity checks,
- Beneficiary validation/Name lookup,
- Risk-based authentication,
- Device and location monitoring,

may be implemented by the Bank.

12.6 Alerts and Customer Notifications

a) SMS/email/push notification alerts shall be sent to customers for:

- Financial transactions,
- Beneficiary addition/deletion,
- Profile modifications,
- Password/PIN changes,
- Other critical activities.

b) Customers shall be encouraged to immediately report unauthorized or suspicious transactions to the Bank.

	12.7 Lost Device and Credential Management a) In case of loss, theft, compromise, or unauthorized access to the mobile device or SIM card, the customer shall immediately inform: • The Bank/branch/helpline • The telecom service provider for SIM blocking. b) The Bank may suspend/block Mobile Banking access until re-registration or reactivation is completed through prescribed verification procedures. 12.8 Security Testing and Vulnerability Management a) Vulnerability Assessment and Penetration Testing (VAPT) of the Mobile Banking Application, APIs, network infrastructure, and connected systems shall be conducted through CERT-In empanelled or qualified security auditors before deployment of the application and thereafter at least annually or at intervals prescribed by regulatory authorities. b) All updates, patches, version upgrades, or major modifications to the Mobile Banking Application shall undergo appropriate security testing and VAPT before deployment into production environment. c) The Bank and service providers, including Kiya.ai, shall ensure timely closure of vulnerabilities and compliance with security observations identified during audits and assessments. 12.9 Regulatory and Security Compliance The Bank shall ensure that Mobile Banking services comply with: • RBI cyber security and digital payment security guidelines, • NPCI operating and security standards, • Information Security Policy of the Bank, • Applicable legal and regulatory requirements relating to electronic banking and payment systems.
13	**Termination, Suspension, and Withdrawal of Facility**
	a) The customer may request termination/de-registration of Mobile Banking and/or UPI facilities at any time by:

- Submitting a written request to the Bank/branch with prior notice of at least 15 days, or using any other mode/channel specified by the Bank through its website, Mobile Banking application, or branch network.

b) The customer shall continue to remain responsible and liable for all transactions initiated or effected through the Mobile Banking/UPI facility prior to actual deactivation or termination of the services.

c) The Bank may, at its sole discretion, withdraw, suspend, restrict, deactivate, or terminate the Mobile Banking/UPI facility, either wholly or partly, temporarily or permanently, with or without prior notice, under circumstances including but not limited to:

- Breach of terms and conditions by the customer,
- Death, insolvency, bankruptcy, or legal incapacity of the customer,
- Account becoming dormant/inoperative as per applicable RBI guidelines,
- Failure to maintain valid KYC compliance,
- Suspicious, fraudulent, unusual, or high-risk transactions,
- Violation of Bank policy, National Payments Corporation of India guidelines, Reserve Bank of India directives, or applicable laws,
- Misuse of the facility for unlawful or prohibited activities including fraud, money laundering, gambling, cybercrime, or unauthorized transactions,
- Compromise or suspected compromise of customer credentials or account security,
- Operational, technical, cyber security, fraud risk management, business continuity, or system integrity concerns,
- Directions issued by regulatory authorities, courts, law enforcement agencies, or statutory bodies.

d) The Bank may temporarily suspend Mobile Banking/UPI services without prior notice for:

- System maintenance,
- Upgrades or patch management,
- Disaster Recovery (DR) drills,
- Security enhancements,
- Vulnerability remediation,
- Network/system failures,
- Emergency situations,
- Regulatory compliance activities.

e) The Bank shall endeavour to provide reasonable notice wherever practicable for withdrawal, suspension, or termination of services; however, immediate action may be

	taken wherever required for security, regulatory, operational, or risk management reasons. f) Closure of all eligible account(s) linked with Mobile Banking/UPI services shall automatically result in termination of the facility. g) Upon termination or suspension of the facility: • Customer access to Mobile Banking/UPI services shall cease, • Pending or disputed transactions shall continue to be governed by applicable terms and conditions, • Rights and obligations accrued prior to termination shall survive until settlement/resolution. h) The Bank shall not be liable for any loss, damage, interruption, or inconvenience arising out of suspension, restriction, or termination of Mobile Banking/UPI services undertaken in accordance with applicable laws, regulatory directions, or security requirements.
14	**Legal Issues**
	a) The Bank shall establish and verify the identity of the customer before providing Mobile Banking and UPI facilities, in accordance with: • Know Your Customer (KYC) requirements, • Customer Due Diligence (CDD) procedures, • Anti-Money Laundering (AML) standards, • Applicable guidelines issued by the Reserve Bank of India and other statutory/regulatory authorities. Mobile Banking facilities shall be enabled only after completion of prescribed customer verification, authentication, and registration procedures as approved by the Bank. b) The Bank recognizes that Mobile Banking and digital payment services involve legal, operational, technology, cyber security, privacy, and fraud-related risks including: • Breach of confidentiality/secrecy, • Unauthorized access, • Phishing and social engineering attacks, • Hacking or malware attacks, • Denial of service, • System/network failures, • Data leakage, • Identity theft, • Fraudulent electronic transactions.

	c) The Bank shall implement appropriate technical, operational, and administrative safeguards including secure technology infrastructure, encryption mechanisms, authentication controls, monitoring systems, cyber security controls, and communication security measures to provide secure, reliable, and reasonably uninterrupted Mobile Banking services. d) The Bank shall maintain appropriate audit trails, transaction logs, and electronic records in accordance with applicable legal and regulatory requirements. Electronic records, transaction logs, authentication records, and system-generated reports maintained by the Bank shall constitute valid evidence of transactions and customer activities unless proved otherwise. e) The customer shall be bound by: • Applicable laws governing electronic banking and payment systems, • Information Technology Act, 2000 and amendments thereto, • Prevention of Money Laundering Act (PMLA), • RBI/NPCI guidelines, • Bank policies, terms, and conditions applicable to Mobile Banking and UPI services. f) The Bank shall have the right to disclose customer information, transaction records, or account-related details: • To regulatory/statutory authorities, • Law enforcement agencies, • Courts/tribunals, • NPCI/payment system participants, • Auditors/service providers, wherever required under applicable laws, regulatory directions, legal proceedings, fraud investigation, dispute resolution, or operational requirements. g) The Bank shall process, store, and share customer data only for legitimate banking, regulatory, fraud prevention, dispute resolution, and operational purposes in accordance with applicable laws and regulatory guidelines. Customer consent shall be obtained wherever required. h) The Bank shall not be liable for any loss or damage arising due to: • Failure of telecom/network/internet services, • System interruptions beyond the Bank's control, • Force majeure events, • Third-party service provider failures, • Customer negligence, • Misuse of credentials,

	• Unauthorized access caused due to customer actions or compromised devices. i) Cyber security incidents, fraud events, or payment system disruptions shall be reported to RBI, NPCI, CERT-In, or other authorities as applicable under regulatory requirements. j) The Mobile Banking and UPI facilities shall be subject to the exclusive jurisdiction of competent courts and applicable laws in India.
15	**Compliant and grievance redressal mechanism to be taken by the Bank**
	15.1 Customer Awareness and Support a) Rajgurunagar Sahakari Bank Limited shall provide adequate education, guidance, and support to customers for safe and secure usage of Mobile Banking and UPI services, with special emphasis on: • Password/PIN security, • Cyber fraud prevention, • Secure digital banking practices, • Safe usage of mobile applications and payment systems. b) The Bank shall establish a Helpdesk/Customer Support facility at its Head Office or designated support center for providing assistance relating to Mobile Banking and UPI services. c) Customers may contact the Bank's Mobile Banking Helpdesk at **8600992100** or through other communication channels notified by the Bank for reporting issues, complaints, unauthorized transactions, or service-related grievances. d) The details of: • Customer support channels, • Grievance redressal mechanism, • Escalation matrix, • Nodal officer details, • Complaint registration process, shall be made available on the Bank's website, Mobile Banking application, and branch premises. e) The above details shall also be communicated to customers during onboarding/registration for Mobile Banking services. f) The Bank shall periodically educate customers regarding cyber security and fraud prevention including:

- Phishing attacks,
- Vishing/caller fraud,
- SIM swap fraud,
- Fake UPI collect requests,
- QR code fraud,
- Remote access application fraud,
- Social engineering attacks,
- Fake customer care scams,
- Safe digital banking practices.

Customer awareness initiatives may be conducted through:

- SMS/email alerts,
- Website notices,
- Mobile Banking application notifications,
- Branch awareness programs,
- Posters/banners,
- Social media/digital communication channels.

15.2 Complaint Registration and Resolution

a) The Bank shall handle customer complaints and grievances relating to Mobile Banking and UPI services promptly, fairly, transparently, and with due priority.

b) Customers may lodge complaints relating to:

- Failed transactions,
- Unauthorized transactions,
- Delayed reversals,
- UPI/IMPS disputes,
- Mobile Banking operational issues,
- Fraud or suspicious activities,
- Service deficiencies.

c) Complaints relating to disputed UPI/IMPS transactions shall be processed through NPCI dispute management/chargeback mechanisms and resolved within timelines prescribed by National Payments Corporation of India and the Reserve Bank of India.

d) The Bank shall maintain records of:

- Complaints received,
- Disputes raised,
- Reversals processed,
- Compensation paid,
- Unresolved grievances,

	for audit, monitoring, and regulatory reporting purposes. 15.3 Customer Compensation a) Failed transaction complaints and customer compensation shall be governed by: • RBI guidelines on Turn Around Time (TAT) and customer compensation for failed transactions, • NPCI operational and dispute management guidelines, • Customer Compensation Policy. b) Compensation, wherever applicable, shall be paid in accordance with prescribed regulatory timelines and conditions. 15.4 Escalation and Ombudsman Mechanism a) In case the customer is not satisfied with the resolution provided by the Bank or the complaint is not resolved within the prescribed timelines, the customer may escalate the matter through the Bank's grievance escalation mechanism. b) Complaints relating to Mobile Banking and digital payment services shall be covered under the RBI Integrated Ombudsman Scheme, as applicable. c) Customers may approach the appropriate Ombudsman authority after exhausting the Bank's internal grievance redressal mechanism or as permitted under applicable RBI guidelines. 15.5 Jurisdiction All disputes arising out of Mobile Banking and UPI services shall be subject to the jurisdiction of competent courts located in Pune, Maharashtra, India.
16	IMPS and UPI Transaction turnaround Time and Customer Compensation Ref. RBI Circular DPSS.CO.PD. No.629/02.01.014/2019-20 dated 20th Sept. 2019 NPCI Circular OC 93 /2019-20 dated 14th October 2019(changed on 22nd Feb 2020)
	In case of the failed IMPS/UPI transactions the Credit amount shall be auto reversed to Customers Account suo moto without waiting for Customer Complaints / Claims along with compensation in case of delay as per time stipulated by RBI/NPCI. 1) The principle behind the TAT is based on the following : a) If the transaction is a 'credit-push' funds transfer and the beneficiary account is not credited while the debit to originator has been effected, then credit is to be effected

	within the prescribed time period failing which the penalty has to be paid to the beneficiary; b) If there is delay in initiation of a transaction at the originator bank's end beyond the TAT, then penalty has to be paid to the originator 2) A 'failed transaction' is a transaction which has not been fully completed due to any reason not attributable to the customer such as failure in communication links, time-out of sessions etc. Failed transactions shall also include the credits which could not be effected to the beneficiary account on account of lack of full information or lack of proper information and delay in initiating a reversal transaction. 3) T is the day of transaction and refers to the calendar date. 4) R is the day on which the reversal is concluded and the funds are received by the issuer / originator. Reversal should be effected at the issuer / originator end on the same day when the funds are received from the beneficiary end.
	Banks Actionable for Unsuccessful Transactions **<u>Remitter / Acquirer</u>** 1) For Declined Transactions (Customer Account is debited and declined at NPCI) it is the remitter responsibility to reconcile and reverse customer account if not done in online within T+1, otherwise remitting Bank has to pay compensation to customer 2) Remitting Bank should reverse the Customer Account on the same day as and when the return\credit adjustments are received otherwise remitting Bank has to pay compensation to customer 3) In case of non-fulfillment of UPI merchant Transactions, acquiring bank should raise return/credit adjustment within 4 calendar days from the transaction date, otherwise compensation shall be debited from acquiring bank and credit same to issuing Bank. **<u>Beneficiary / Issuer</u>** **1)** Bank as a Beneficiary should credit the customer's account within T+1 day (if not credited online) otherwise customer account has to be credited with compensation. **2)** If the amount cannot be credited due to any reason same has to be returned to remitting Bank UPI & IMPS transactions by T+1, otherwise NPCI shall debit the beneficiary Bank and credit to remitting Bank. Remitting Bank should credit their Customer Account (Transaction Amount+ Compensation) on the same day. If delayed then remitting bank has to pay compensation to customers **3)** For UPI merchants transaction acceptance by acquiring Bank for chargeback or pre-arbitration (including deferred charge back cycle) should be done within 4 days then NPCI shall debit the acquiring bank and credit issuing Bank transaction amount+ compensation. Issuing bank should credit the amount to customers account on the same day or latest by 5^{th} day from the transaction day. If delayed then issuing Bank shall pay additional compensation to the customer

Changes in Dispute Processing

Conditions for customer compensation shall be calculated from the transaction date to the customer account credited / reversed date if it is within T+1 for P2P and T+5 for P2M customer compensation will not be applicable.

For IMPS and UPI P2P Transactions

Adjustment Type	Within T+1	*After T+1
Chargeback Accept / Deemed Accept	NA	Applicable
Pre-Arbitration Accept	NA	Applicable
Pre-Arbitration Deemed /Deemed Accept	NA	Applicable
Arbitration Accepted	NA	Applicable
Deferred Chargeback Accept\Deemed Accept	NA	Applicable
Deferred Pre-Arbitration Accept \ Deemed Accept	NA	Applicable
Deferred Arbitration Accept	NA	Applicable

*T+1 indicate transaction next day for UPI and for IMPS

For UPI Merchants Transactions

Dispute Name	Within T+4	*After T+4
Return \ Credit Adjustment	NA	Applicable
Chargeback Accept\Deemed Accept	NA	Applicable
Pre-Arbitration Accept /Deemed Accept	NA	Applicable
Arbitration Accept	NA	Applicable
Deferred Chargeback Accept\Deemed Accept	NA	Applicable
Deferred Pre-Arbitration Accept \ Deemed Accept	NA	Applicable

	Deferred Arbitration Accept	NA	Applicable

** T+4 indicates 4th day from the day of the transaction

a) Compensation shall not be applicable for wrong credits or fraudulent transactions
b) Where merchant \acquirer failed to initiate credit adjustment /refund, if the customer lodges the complaint with the issuing Bank, issuing Bank to initiate a chargeback with specific MMT (member message text) as Account debited but confirmation not received at merchants locations to identify dispute arising due to such failed transactions.

17 **Customer Liability for Unauthorized Electronic Banking Transactions**

A) Systems and Procedures

1) Bank has appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by its customers;
2) Bank has robust and dynamic fraud detection and prevention mechanism;
3) Bank has put in place mechanism to assess the risks resulting from unauthorized transactions and measure the liabilities arising out of such events;
4) Bank is continuously taking appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom;
5) Bank will at regular intervals advise customers on how to protect themselves from electronic banking and payments related fraud

B) Reporting of Unauthorized Transactions

1) All the Customers of the Bank shall mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions.
2) Bank shall send SMS alerts mandatorily to all Customers and email alerts shall be sent wherever registered. The customers must notify their bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction.
3) Customers shall report the Unauthorized Transaction at Branches or shall send the email to the Bank on email id report at any branch of the bank.
4) Customers shall inform the bank immediately of the unauthorized transactions and failure to do so shall increase the liability or risk of loss to the bank/ customer.
5) Customer reporting the unauthorized Mobile Banking/UPI Transaction involving fraud must file FIR with Local Police Station and submit the copy of the FIR to the Bank.

Limited Liability of the Customer

D) Zero Liability

1) In case of Unauthorized Transaction 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 the bank within three working days of receiving the communication from the bank regarding the unauthorized transaction.

E) Limited Liability of the Customer

1) A 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, the customer will bear the entire loss until he reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.
   (ii) In cases where the responsibility for the 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 (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in below Table, whichever is lower.

Maximum Liability of the Customer under Para 9 (E) and RBI circular dated 14th December 2017 Para 7 (ii)		
Sr. No.	**Type of Account**	**Maximum Liability**
1	Basic Savings Account	Rs.5,000/-
2	• 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 • Credit cards with limit up to Rs.5 lakh	Rs,10,000/-
3	• All other Current/ Cash Credit/ Overdraft Accounts	Rs.25,000/-

	• Credit cards with limit above Rs.5 lakh	

F) Summary of Customer Liability

Overall liability of the customer in third party breaches, as detailed in paragraph D and paragraph E above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized in Table given below

Summary of Customers Liability		
Sr. No.	**Time taken to report the fraudulent transaction from the date of receiving the communication**	**Customers Liability**
1	Within 3 working Days	Zero Liability
2	Within 4 to 7 working Days	The transaction value or the amount mentioned in Table given in E above whichever is lower
3	Beyond 7 working days	As per Banks Board Approved Policy

G) Customers Account will be credited within 10 days from the Receipt of the Compliant in above cases.

H) Reporting of the Transactions Beyond 7 working Days

In case the Customer Report the unauthorized transaction after 7 working days Customer Liability shall be 50% of the Transaction value or Rs. 10,000/- whichever is higher.

I) Reversal Timeline for Zero Liability / Limited Liability Customer

1) On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorized 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 unauthorized transaction.

	2) Bank shall within 90 days from the date of the complaint shall resolve Customer complaint and liability of the customer, if any, established and the customer shall be compensated as per provisions of paragraphs F above. In cases where liability is not established or customer is not compensated within 90 days from the date of complaint Customer will be compensated as per clause F above immediately.
18	**DR Drill**
	Bank shall carry out DR drill for UPI and IMPS Switch from Infrasoft (Kiya.ai) being ASP (Application Service Provider) for all UPI and IMPS infrastructure at least once every six (6) months (half-yearly) as per financial year. DR drill and the rollback to PR should be carried out during nighttime between 00:00 HRS and 06:00 HRS, so that customer impact is minimized. Bank shall share the DR drill plan with NPCI at least a week in advance along with plan downtime. NPCI operating circular vide NPCI/ONLINEOPS/2023-24/001 dated 18th Sep 2023 for details.
19	**EFRM System (Fraud Reporting)**
	Bank shall register for EFRM facility of the NPCI and all the transactions reported in EFRM shall be monitored and shall be verified with Customer on on-going basis. Frauds reported if any by the Customer shall be reported on EFRM portal of NPCI
20	Customer Application Form at branch level for enrollment for Mobile Banking shall be as per Annex. A to the policy
21	GOVERNING LAW: This policy shall be governed and construed in accordance with the laws of India and any dispute or differences arising out of or in connection with the Facility shall be subject to the exclusive jurisdiction of the Courts at Pune. Rajgurunagar Bank accepts no liability whatsoever, direct or indirect for non-compliance with the laws of any country other than that of India. The mere fact that the Facility can be accessed by a Customer in a country other than India does not imply that the laws of the said country govern this policy and / or the operations in the account(s) of the Customer and / or the use of the Facility

Mobile Banking & UPI Policy

Policy has been approved by Board of Director Meeting Dated 24/03/2026 Resolution Number 5(19)-4 .

Assistant General Manager I.T.	**General Manager**
Chief Executive Officer	**Chairman**