Digital Banking Policy

Table of Contents

ABBREVIATIONS

ABBREVIATION	DESCRIPTION
AML	Anti Money Laundering
AS	Accounting Standard
ATM	Automated Teller Machine
CDO	Chief Digital Officer
CFT	Combating Financial Terrorism
CIC	Credit Information Company
CIO	Chief Information Officer
CISO	Chief Information Security officer
CRM	Cash Recycler Machine
CRMC	Credit Risk Management Committee
CUG	Closed User Group
CVV	Card Verification Value
DBD	Digital Banking Department
DBU	Digital Banking Unit
DCRD	Digital Channel Reconciliation Department
DPSC	Digital Payment Security Controls
eFRMS	Electronic Fraud Risk Management System
GCC	General Credit Card
ICCW	Interoperable Cardless Cash Withdrawal
IMPS	Immediate Payment Service
ISE	Inspection for Supervisory Evaluation
ITSC	Information Technology Strategy Committee
KYC	Know Your Customer
MCC	Merchant Category Code
MDR	Merchant Discount Rate
NCMC	National Common Mobility Card
NEFT	National Electronic Fund Transfer
ODR	Online Dispute Resolution
ORMC	Operational Risk Management Committee
PII	Personally Identifiable Information
POS	Point of Sale
PPI	Prepaid Payment Instrument
QR	Quick Response
QRT	Quick Response Team
RPA	Robotic point Automation
RPO	Recovery Point Objective
RTGS	Real Time Gross Settlement
RTO	Recovery Time Objective
SOP	Standard Operating Procedure
SSL	Secured Socket Layer
TD	Technical Decline
TLS	Transport Layer Security
UAT	User Acceptance Testing
UPI	Unified Payment Interface
VCC	Virtual Credit Card

1. Introduction:

A Digital Banking Policy is vital to draw and implement strategies for leveraging the tools of digital products to improve internal operations, retaining and expanding our position in the banking system, enhancing the ability to deliver on our core competencies and ensuring competitiveness by providing innovative products and services at competitive costs. Digital products are the effective tools for increasing digital penetration efficiency and profitability.

The Bank wishes to use Digital products to enable the various business activities of retail, corporate, trade and treasury with the objective of providing a strong, robust and efficient banking environment for offering the services as per the demands of the customers & the regulatory requirements.

With a view to meeting the business requirements and achieving the desired Digital goals as per the Bank's plan and keeping in view the changing global scenario especially in the financial sector and its impact on the banks, it is proposed to introduce the Digital Banking Policy for the Bank and define the broad policy directives and measures.

The following chapters will be part of Digital Banking Policy:

a. Chapter I – Debit Card
b. Chapter II – PPI Issuance and Operations
c. Chapter III – Merchant Acquisition
d. Chapter IV – ATM and Recycler
e. Chapter V - UPI
f. Chapter VI - QR Code
g. Chapter VII - WhatsApp Banking
h. Chapter VIII - Digital Signature
i. Chapter IX - FASTag
j. Chapter X - Digital Channel Reconciliation
k. Chapter XI – Digital Banking Unit
l. Chapter XII – Mobile Banking
m. Chapter XIII – Internet Banking
n. Chapter XIV - Credit Card
o. Chapter XV – Robotic Process Automation
p. Chapter XVI – Product Testing

2. Mission Statement:

Digital Technology as a business *'enabler'* shall be put to optimal use in the Bank for satisfying the needs of both 'internal' and 'external' stakeholders; enabling the Bank to be the best among the peer banks for facing the competition in the area of business growth, customer retention & expansion and enhancing profitability through process reengineering.

3. Objectives:

a. To define Bank's broad guidelines and thrust areas for use of Digital Products to create "Digital Bank within the Bank" and to make best Bank among the peer Banks in tandem with the '*Vision Document'* of the Bank.

b. To establish state-of-the-art digital infrastructure in the Bank not only to help in the internal housekeeping and minimizing business risk, but also to ensure our competitiveness by providing innovative products and services at competitive costs.

c. To implement customer-centric digital products and services for enabling the Bank to cater to the needs of the customers, enhance customer experience as well as to fulfill the regulatory requirements.

d. To pursue Business Process Re-engineering activities and re-define outdated legacy process and systems for improving efficiency and profitability with cost optimization.

e. Leveraging new age Fintech platform to extend personalize services to customers.

f. To fulfill obligations towards '*social banking'* through use of digital products.

4. Scope of the Policy:

The scope of this Policy will cover all locations of the Bank including all digital assets, digital products, business processes supported by digital products and all employees of the Bank as well as other offices including associates, joint ventures, subsidiaries in India and abroad (if any).

This Digital Banking Policy is intended to provide a framework for secure and reliable digital banking services. It shall be supported by additional detailed procedures and guidelines that are developed and maintained by the digital banking department.

5. Definitions:

a. **Digital Banking:** Digital Banking refers to present and future electronic banking services provided by a licensed bank for the execution of financial, banking and other transactions and/or orders/instruments through electronic devices / equipment over web sites (i.e. online banking), mobile phones (i.e. mobile banking) or other digital channels as determined by the bank, which involve significant level of process automation and cross-institutional service capabilities running under enhanced technical architecture and differentiated business model / strategy.

b. **Digital Banking Segment:** A Digital Banking Segment, for the purpose of disclosure under Accounting Standard 17 (AS-17), is a sub-segment of the existing 'Retail Banking' Segment which will now be sub-divided in to (i) Digital Banking and (ii) Other Retail Banking. The business involving digital banking products acquired by DBUs or existing digital banking products would qualify to be clubbed under this segment.

c. **Digital Banking Products:** Digital Banking products and services would generally mean those financial products/services whose designs and fulfilments have nearly end-to-end digital life cycle with the initial customer acquisition / product delivery necessarily taking place digitally through self-service or assisted self-service.

d. **Digital Business Zone (DBZ):** Digital Business Zone refers to the Zone which will be responsible for the maintenance, upgradation, and promotion of digital products, along with targeted customer outreach programs to drive adoption and business mobilization. The primary objective is to increase the Bank's share of digital

business, thereby reducing branch workload and providing a superior customer experience

6. Thrust Areas:

The Digital Banking Policy is drawn in recognition of the fact that it meets the Bank's overall business context and corporate plan, it supports the strategic digital initiatives of the Bank. The opportunities enabled by digital products can shape the Business Strategy of the Bank, such as new delivery channel opportunities, digital products etc.

Keeping this in mind, the following thrust areas have been identified under digital banking;

a. Work towards enhancement in the Performance of ATMs/Recyclers/Passbook Kiosks/Multifunction Kiosk/Account Opening Kiosk, Point of Sale (POS) etc.,

b. Implementation / Extension of GOI/NPCI Initiatives -
   - BHIM UPI
   - BHIM Aadhaar Pay
   - Bharat QR Code
   - Bharat Bill Payment System (BBPS) etc.

c. Compliance to various advisories issued by RBI and other regulatory authorities.

d. Digital banking Department shall be responsible for implementing and managing various digital initiatives for the Bank. Department shall also be responsible for managing and enhancing the existing digital channels like ATM/Recycler, Mobile Banking, Internet Banking, WhatsApp Banking, Multi-function Kiosk, Passbook Kiosk, FASTag, QR Code, UPI, Debit Cards, Credit Cards, POS, DBUs etc. The Dept. will also endeavor to add digital channels viz. Lifestyle Banking, Digital journey, etc. in tandem with market.

e. Increasing digital footprint for various digital channels like Internet Banking, Mobile Banking, WhatsApp Banking, FASTag, QR codes, Maha UPI/ BHIM, Digital Banking Units etc., to increase the percentage of e-transactions.

f. Bank shall issue SOP for new product and it should cover the objective, base of the process and detailed procedure. All SOPs shall be reviewed on yearly basis and shall remain valid for a period of one year or until reviewed after one year (in case not reviewed).

The policy aims to ensure customer trust, data protection, and compliance with regulatory requirements. All employees, customers, and stakeholders must adhere to this policy when using or providing digital banking services.

7. Compliance and Regulatory Requirements

a. Regulatory Compliance:

   i. All digital banking services/products shall comply with applicable laws, regulations, and guidelines set forth by regulatory authorities, such as the Reserve Bank of India (RBI).

ii. The DBD shall maintain records and documentation to demonstrate compliance with regulatory requirements.
iii. Respective team/officials shall ensure the compliance of regulatory requirements within stipulated timeline defined by the regulator. In case of any delay/extension of timeline, department shall obtain necessary approval from competent authority.
iv. Bank shall ensure compliance with Section 3: ATM/POS/Card payment security and section 11: securing payment ecosystem RBI CSITE Advisory.

b. Reporting and Auditing:

i. Regular audits of the digital banking processes and controls shall be conducted to ensure adherence to policies and regulatory requirements.
ii. Incident reporting mechanisms shall be adhered as per Incident Management Policy/BCP Policy of the Bank to promptly report any security breaches or data incidents to the appropriate authorities.
iii. The downtime in case of critical channels beyond usual prescribed timelines shall be reported to regulator through CISO cell as per advisory from RBI/NPCI/CSITE, etc.

c. Communication and Awareness:

i. Regularly communicate updates and changes to the digital banking policy to employees, customers, and stakeholders.
ii. Ensure that employees and customers are aware of their responsibilities and obligations as outlined in the policy.
iii. Provide regular training and awareness programs for bank employees to educate them about digital banking security best practices, policies, and procedures. b. Employees should be familiar with their roles and responsibilities in maintaining digital banking security and protecting customer data.

d. Customer Support:

i. Efficient and timely customer support should be available to address any digital banking-related queries, issues, or complaints.
ii. Multiple support channels (e.g., phone, email, chat) should be provided for customer convenience.

e. Customer Education:

i. Regular educational campaigns should be conducted to raise customer awareness about safe digital banking practices.
ii. Educational materials, tutorials, and security tips should be made readily available to customers.

f. Monitoring and Assessment:

i. Ongoing monitoring of digital banking systems, networks, and applications should be conducted to detect and respond to potential vulnerabilities or threats.
ii. Regular risk assessments and security audits should be performed to identify areas of improvement and address emerging risks.
iii. Monitoring and pro-active enhancement of all digital Infrastructure of the Bank duly ensuring BCP & technology resilience i.e. Digital Banking wing will also envisage future enhancement of Digital infranets duly considering system utility

vis-à-vis growth in digital transactions anticipated for future. The requirement of such enhancement shall be brought to the notice of ITSC/Board timely in coordination with IT Deptt. Periodically by DBD.

Technical & Business Declines in case of critical digital channels shall be monitored regularly to minimise the same & declines reported higher than normal levels shall be analysed. A periodical note of analysis of TD shall be placed to ED.

g. Privacy and Data Protection

i. Data Collection and Consent:
   a) Clear and transparent policies must be established regarding the collection, storage, processing, and sharing of customer data.
   b) Consent should be obtained from customers for data usage, and they should have the ability to manage their consent preferences.

ii. Personally Identifiable Information (PII):
   a) PII must be protected using appropriate security measures, and access should be granted on a need-to-know basis.
   b) PII should only be used for legitimate banking purposes and not shared with third parties without customer consent, except as required by law.

iii. Bank shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.

h. Data Retention:

i. Data retention policies must be established to determine the duration for which customer data is retained.
ii. Obsolete or unnecessary data must be securely disposed of in accordance with regulatory guidelines.

i. Security Measures

i. User Authentication:
   a) Two-Factor Authentication (2FA) must be implemented for all customer logins and high-risk transactions.
   b) Strong password requirements, including complexity, length, and periodic password changes, must be enforced.
   c) Additional security measures such as biometric authentication and device recognition should be considered.

ii. Data Encryption:
   a) All customer data transmitted over digital channels must be encrypted using industry-standard encryption protocols.
   b) Encryption should also be applied to data at rest, ensuring the protection of sensitive information stored within the bank's systems.

iii. Secure Communication:
   a) Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols must be employed for secure communication between the bank's servers and customer devices.

b) Regular vulnerability assessments and penetration testing should be conducted to identify and address any weaknesses in the bank's digital infrastructure. As per ISSP Policy the frequency for conducting VA & PT is quarterly and as per the criticality of the product.

j. Fraud Detection and Prevention:

i. Digital Channels (if applicable) including Credit Card shall be integrated with Bank's eFRMS platform to identify and prevent fraudulent activities.
ii. Real-time monitoring of customer transactions, anomaly detection, and automated alerts should be in place.
iii. Regular customer education and awareness programs should be conducted to help customers recognize and report potential fraud attempts.

k. Cyber Security:

i. Bank of Maharashtra believes in providing services to its customers in the safest and secure manner keeping in mind that data protection for its customers is as important as providing quality banking services across the spectrum. The CIA triad of Confidentiality, Integrity, and Availability is at the heart of building a comprehensive information security framework
ii. The Bank also undertakes campaigns to create awareness among customers on security aspects while banking through digital channels.

l. Device Policy:

Bank shall enforce security policy for mobile devices which will be divided into four stages i.e. sensitive data isolation, security policy formulation, security policy testing and security policy execution. The mobile apps shall be installed and executed only after meeting baseline requirements.

m. Application Life Cycle:

Bank shall include all stages in application lifecycle i.e. planning, design, build, release, maintenance, and updates, as well as the replacement and retirement of the application when the need arises. Bank shall also ensure security in all stages of the lifecycle and shall adopt thread-modeling approach during application lifecycle management.

The different stages in lifecycle are the identification stage, the assessment stage, the design phase, the implementation stage, the protection stage, and the monitoring stage. Bank shall maintain only one application / mobile app version (excluding overlap period) on a platform /OS. Bank shall deactivate older application / mobile app version in a phased and time-bound manner.

8. Limit Review for Digital Channels:

The limit of Debit card products, Credit Card products, MB, IB, IMPS, UPI, BHIM QR, Bharat QR, FASTag and any other digital product shall be reviewed by the Digital Products Limit Review Committee annually. However, a review shall be done at any time in case of any specific requirement mandated by Regulators, GOI, Bank's Management or in case of exigencies.

9. Rewards & Recognitions:

For recognizing the exceptional contribution/achievements by Bank officials and increasing the penetration of digital footprints, Bank may offer, financial or non-financial rewards & recognition. The different types of rewards & recognition initiatives are as under:

a. Certificate of Appreciation
b. Employee of the Month Award
c. Employee of the Year Award
d. Campaign specific Incentives
e. Incentives for innovations and initiatives
f. Rewards for customers to increase the usage & penetration of Bank's Digital Products.

It will provide healthy competitive environment to take initiative, be creative and popularize Bank products among customers.
The necessary budgetary provisions shall be made in IT Budget of the Bank. The Nature of rewards and recognition shall be approved by the In-Charge of Digital Banking/Chief Digital Officer of the Bank.

10. Digital Organization Structure:

a. The General Manager/ Deputy General Manager/In-Charge of Digital Banking shall be the **Chief Digital Officer (CDO)** of the Bank.

11. Internal control and monitoring systems:

Inspection and Audit department, periodically (at least yearly) will audit the adequacy and effectiveness of processes and controls carrying out of the operation of Digital Banking products and report on this shall be placed before ACB.

Risk assessment emanating from Digital Banking operations such as reputational risks, operational risks, market risks etc., shall be carried out by IRM department on half yearly basis and Risk assessment report for every department are placed by IRM deptt. to ORMC through RCSA.

The bank should undertake a comprehensive review of all applications to assess the need of masking/encrypting personally identifiable information (PII) (i.e. at rest, in-use and in-transit) and implement appropriate controls.

The bank should undertake risk assessment of all APIs, conduct VA/PT, Source Code audit, API audit and General process audit wherever applicable before go-live of any Digital Banking Products.

Digital Banking Department shall review newly introduced features/ services/ applications and submit the report to ITSC of Board in ensuing quarterly meeting.

Rollback plan shall be in place in case of any adverse observations after production movement of any new application/ product/ enhancement.

In case of any incident/ major activities which causes disruption of any facility/ services affecting customers, Digital Banking Department shall inform the same to QRT through IRM.

Banks shall obtain certificate from application vendors stating that new products, updates, upgrades are developed following secure coding practices. The application architecture shall

be tested to safeguard the confidentiality and integrity of data being stored, processed and transmitted.

Password policy as per ISSP policy of the Bank shall be referred for payment channels like IB, MB, UPI for frequency of change of password, length, PIN, TPIN, etc.

Bank shall have a digital dashboard of applications/products (if applicable) for monitoring of applications/products and generation required reports.

DBD will undertake periodical review of registered customers beyond 1 years period without any transactions and take suitable action to deactivate / escalate to users to avoid any misuse of digital channels in case of various platforms viz (MB, IB, UPI, Cards etc.)

The access control & admin rights available to vendor's /Bank officials shall be reviewed on quarterly basis and necessary resets of passwords shall be undertaken as per ISSP /IT policy guidelines.

Bank shall have availability of adequate requisite infrastructure e.g. human resources, technology, etc. with necessary back up.

Bank shall have necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product/ services offered.

Bank shall ensure payment product is built in a secure manner offering robust performance ensuring safety, consistency and rolled out after necessary testing for achieving desired FSP.

Bank shall ensure Minimal customer service disruption with high availability of systems/ channels (to have minimal technical declines).

Bank shall ensure adequate and appropriate review mechanism followed by swift corrective action, in case any requirements is hampered or having high potential to get hampered.

12. Outsourcing of various services:

Bank shall ensure adherence to the guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services which are covered under Bank's outsourcing policy and amended from time to time.

13. Confidentiality of customer information

Bank shall not reveal any information relating to customers to any other person or organization without obtaining their explicit consent, with regard to the purpose/s for which the information will be used and the organizations with whom the information will be shared. Bank shall ensure strict compliance to the extant legal framework on data protection. Further, in case where the customers give explicit consent for sharing the information with other agencies, Bank shall explicitly state and explain clearly to the customer the full meaning/implications of the disclosure clause. The information sought from customers shall not be of such nature which will violate the provisions of law relating to maintenance of secrecy in the transactions. The Bank shall be solely responsible for the correctness or otherwise of the data provided for the purpose.

No entity shall be permitted to access any details of customer's accounts that may violate the card-issuer's secrecy obligations.

14. Customer protection and grievance redressal framework

Bank shall disclose all important terms and conditions in clear and simple language (preferably in English, Hindi and the local language) to the holders while issuing the instruments. These disclosures shall include:

a. All charges and fees associated with the use of the instrument; and
b. The expiry period and the terms and conditions pertaining to expiration of the instrument.

Bank shall create sufficient awareness and educate customers in the secure use of the PPIs, including the need for keeping passwords confidential, procedure to be followed in case of loss or theft of card or authentication data or if any fraud / abuse is detected, etc.

Bank shall provide an option for the PPI holders to generate / receive account statements for at least past 6 months. The account statement shall, at the minimum, provide details such as date of transaction, debit / credit amount, net balance and description of transaction. Additionally, the Bank shall provide transaction history for at least 10 transactions.

15. Information System Audit:

a. Banks shall be guided by RBI circulars DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011, DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated June 02, 2016, Bank's Cyber Security Policy and other relevant circulars on the subject, as amended from time to time.

b. Bank shall also be guided by the RBI circular DBS.CO/CSITE/BC.11/33.01.001/2015-16 on Cyber Security Framework in Banks dated June 02, 2016, which inter alia, covers requirements for mobile-based applications. Digital Banking Department will get the Information System Audit done through Inspection and Audit Department.

c. The scope of the Audit shall include the following:

   i. Security controls shall be tested both for effectiveness of control design (Test of Design – ToD) and control operating effectiveness (Test of Operating Effectiveness – ToE).
   ii. Technology deployed so as to ensure that the authorised payment system is being operated in a safe, secure, sound and efficient manner.
   iii. Evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key applications, disaster recovery plans, training of personnel managing systems and applications, documentation, etc.
   iv. Evaluating adequacy of Information Security Governance and processes of those which support payment systems.
   v. Compliance as per security best practices, specifically the application security lifecycle and patch / vulnerability and change management aspects for the authorised system and adherence to the process flow approved by RBI.
   vi. Comment on the deviations, if any, in the processes followed from the process flow submitted to competent authority while seeking authorisation.
   vii. Application Life Cycle Security: The source code audits shall be conducted by professionally competent personnel / service providers or have assurance fromapplication providers / OEMs that the application is free from embedded malicious /fraudulent code.

viii. Security Operations Centre (SOC): Integration of system level (server), application level logs of mobile applications with SOC for centralised and co-ordinated monitoring and management of security related incidents.
ix. Anti-Phishing: Bank shall subscribe to anti-phishing / anti-rouge app services from external service providers for identifying and taking down phishing websites / rouge applications in the wake of increase of rogue mobile apps / phishing attacks.
x. Risk-based Transaction Monitoring: Risk-based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system.
xi. Disaster Recovery: Bank shall consider having DR facility to achieve the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) for the all the systems/applications to recover rapidly from cyber-attacks / other incidents and safely resume critical operations aligned with RTO while ensuring security of processes and data is protected.
xii. The above scope is indicative & the same shall be followed as per audit needs as per latest ISSP policy

16. Vendor Risk Management:

a. Bank shall enter into an agreement with the service provider that amongst others provides for right of audit / inspection by the regulators of the country;
b. RBI shall have access to all information resources (online / in person) that are consumed by service provider, to be made accessible to RBI officials when sought, though the infrastructure / enabling resources may not physically be located in the premises of service provider;
c. Bank shall adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders;
d. Bank shall review the security processes and controls being followed by service providers regularly;
e. Service Agreements of Bank with service provider shall include a security clause on disclosing the security breaches if any happening specific to issuer's ICT infrastructure or process including not limited to software, application and data as part of Security incident Management standards, etc.
f. The above terms are indicative and the details be referred to Vendor Management policy within IT policy

17. Right to Audit:

Bank/ Regulator or any other party authorized by the Bank can conduct audit of Aggregator/Partner or third party agent.

18. Governing Law and Jurisdiction:

The laws of India shall govern these terms and conditions and/or the operations in the Account(s) maintained with Bank. Any legal action or proceedings arising out of these Terms shall be brought under the exclusive jurisdiction of the courts or tribunals/forums located in Pune, India only and irrevocably submitting themselves to the jurisdiction of that court or tribunal.

These terms & Conditions are subject to periodic updation. The User/Partner understands that Bank may amend the above terms and conditions at any time without any notice or assigning any reason whatsoever and such amended Terms and Conditions will there upon apply to and be binding on the User/Partner.

Bank of Maharashtra may, however, in its absolute discretion commence any legal or proceedings arising out of these Terms and Conditions in any other court, tribunal or other appropriate forum, and the user/partner hereby consents to the jurisdiction.

19. Policy Review and Updates:

The policy shall be reviewed on yearly basis and shall be approved by the Board of Directors of the Bank and shall remain valid for a period of one year from such approval or until reviewed/ policy enforce after one year (in case not reviewed). However, Bank's MD & CEO will have delegated power for extension of due date by 3 months in case of exigencies.

20. References:

1. RBI/DPSS/2021-22/82.CO.DPSS.POLC.No.S-479/02.14.006/2021-22 dated 21/08/2021- Master Directions on Prepaid Payment Instruments (MD-PPIs)
2. Master Direction on Outsourcing of Information Technology Services dated 10.04.2024
3. Cyber Security Framework in Banks dated 02.06.2016
4. Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices dated 07.11.2023
5. Master Direction on Digital Payment Security Controls dated 18.02.2021
6. Storage of Payment System Data DATED 06.04.2018
7. ISE Audit 2024 & 2023

Chapter I

Debit Card

1. Introduction:

The Debit Card Policy, hereinafter referred to as the "Policy", is aimed at providing guidance to the employees and customers of Bank of Maharashtra (hereinafter called the "Bank"), and to lay down the systems and controls expected for managing the debit card issuance.

The policy documents govern the current business strategy of the Bank with regard to issuance of Debit Cards to its esteemed customers. The policy also lays out the various charges and terms associated with Debit Card usage.

Debit Card is a physical or virtual payment instrument containing a means of identification, linked to a Saving Bank/Current Account which can be used to withdraw cash, make online payments, do PoS terminal transactions, fund transfer, Mobile Banking registration, UPI registration etc. subject to prescribed terms and conditions

2. Governance and Intended Audience:

This policy is intended for the concerned employees within the Bank, who are dealing with debit card management & issuance. The Digital Banking shall be responsible for ensuring that the policy is updated with regard to the applicable rules and regulations of the Bank and also of various regulators, including the Reserve Bank of India.

The IT Department shall be responsible for maintaining the infrastructure related to debit card issuance and shall work with the concerned departments to ensure that features proposed to the customers are implemented correctly within the various systems of the Bank.

The Digital Banking Department shall oversee the debit card supply to various Zones/Branches. Procurement Wing shall do the procurement as per business requirement.

Proper need based supply & proper safe keeping of debit card in the Zones & Branches shall be ensured by Digital Banking dept.

3. Important Specifications of a Debit Card:

The Debit Card specification shall comprise of 16 digit card number linked to customer's savings/ current bank account. First 6 digits represent Bank's identification number (BIN), next 4 digits indicates card product code, next 5 digits indicates sequence number and last 1 digit indicates check digit.

The other specifications shall be as under:

a. Name of the Person: Person authorized to use the card. This field is present only on personalized card.

b. Valid Date: It is in mm/yy format. The card is valid till the last day of the month.

c. Card Verification Value (CVV) /CVV2: The CVV (present in track 2 of card) data is transmitted automatically when the consumer swipes or dips their card.

d. CVV2 code is a three-digit number printed on the back of every debit card. This is used for validation of online transaction.

e. Magnetic Strip: Important information regarding the debit card is stored in electronic format on the magnetic strip.

f. EMV Chip Card: EMV stands for Europay, MasterCard and Visa. EMV is a global standard for credit and debit payment cards based on chip card technology. EMV Chip Card protects against counterfeit (skimming) card fraud.

g. CVV (Integrated Chip Card - Card Verification Value): This is the code stored in the card's chip (EMV)

4. Personal Identification Number (PIN):

The PIN shall be 4-digit secret number/code, which is given to the customer at the time of issuing a debit card for the purpose of security.

Bank shall make aware the customer for changing the pre-set PIN before the first transaction on the debit card.

Bank shall make use of Green-PIN through Mahabank ATMs in order to provide quick PIN generation/reset facility to the customers.

5. Types of Debit Cards:

Bank issues various types of personalized and non-personalized debit cards. These cards shall be allowed to use at ATM, POS & over the Internet for online usage. Customers are required to submit requisite application form for Debit card, duly signed. Debit cards shall be primarily issued against personal or business use. Typically, a debit card is only issued against a savings account or current account. A Single card can be linked to multiple accounts under single CIF. Details of various debit card variants are as below:

a. **Rupay Debit Cards:** Rupay Debit Card is an Indian version of debit card. It is very similar to international cards such as Visa/Master. Currently, the Bank is offering various variants of Rupay Debit cards to its customers.
b. **Visa Debit Cards:** Visa Debit is a major brand of debit card issued by Visa. Currently the Bank is offering two variants of Visa Debit Card i.e. VISA EMV Card and VISA Purple Cards.
c. **National Common Mobility Card (NCMC):** National Common Mobility Card (NCMC) is prepaid instrument and a dual interface (Contact & Contactless) EMV card. This is aimed at low value payments for various segments e.g. transit, smart cities, toll, parking and other low value merchant payments in addition to the normal day to day retail payments.)
d. **Prepaid Cards:** Prepaid payment instruments are payment instruments that facilitates purchase of goods and services, against the value stored on such instruments. The value stored on such instruments represents the value paid by the card-holders by debiting the bank account.
e. **Virtual Cards:** A virtual card is an electronic form of a physical debit card made for Card Not Present (CNP) transactions. It has its own unique card number, expiration date and CVV, which can be used to initiate online transactions.

Bank shall provide the virtual card facility through any bank's mobile applications. The virtual cards shall contain all the same information as physical debit cards and can be used for making purchases, buying goods/ services online, contactless payment or for MB, UPI registration purpose.

6. Debit Card Fees:

The Bank shall decide the fees and charges as and when required related to issuance of debit card. The debit card fees are covered under services charges booklet issued every year by planning department.

7. Services Available on Debit Card:

With Debit Card bank shall provide services like Pre-defined preferred amount, Cash Withdrawal, Balance Enquiry, Mini Statement, Change of PIN, Transfer of Funds within BOM – Card to Card and Card to Account, Aadhaar Number Seeding on Bank's ATMs and services like Cash Withdrawal, Balance Enquiry and Mini Statement on other Bank's ATMs (NFS Network)

At POS terminals the services like Bill payments, Cash at PoS etc. shall be provided. For online usage Debit card shall be used for online purchase, ticket booking (Railway, Movie, Bus etc.), payment of Bills etc. customer can use debit card.

For all such transactions, SMS/e-mail alerts to the cardholders shall be given.

Any addition /deletion/enhancement in services shall be done after approval of CDO/GM digital banking and shall be put up to ORMC on quarterly basis.

8. Usage Policy:

The Debit Card shall be governed by the below terms and conditions:

a. The Cardholder should at all times ensure that the Card is kept at a safe place and under no circumstances whatsoever, should allow the Card to be used by any other individual.

b. The Cardholder should sign the Card immediately upon receipt.

c. The Cardholder should change the PIN assigned by the Bank on first usage and choose another PIN as a safety measure for secured usage of the Card.

d. The Cardholder shall be responsible for all facilities granted by the Bank and for all related charges and shall act in good faith in relation to all dealings with the Card and the Bank.

e. The Bank reserves the right to change the types of transactions supported by the Card subject to a notice being given to the Cardholders by way of sending SMS, displaying notice on Bank's website, displaying message on board of Bank's branches.

f. Below shall be the notice period in the event of changes to the types of transactions:

   i. Non-financial: 3 days
   ii. Financial: 7 days
   iii. Emergency: Immediately as per Change Management Process

g. The Cardholder should notify the Bank immediately of any error or irregularity in maintaining the account/ card by the Bank at Mahaseva or by way of written communication to any of the branch of the Bank or such other mode as may be acceptable to the Bank.

h. International Debit Cards can be used only for permissible current account transactions under the Foreign Exchange Management Act (FEMA), 1999 (and/or any other applicable laws) and the item-wise limits as mentioned in the Schedule III to the Government of India Notification No.G.S.R. 381(E) dated May 3, 2000, as amended from time to time, are equally applicable to payments made through use of these Cards.

i. The default transaction limit for International usage, domestic E-commerce and contactless payments is set to zero. Customer shall make an explicit request for enhancing their limits.

j. International Debit Cards can be used on Internet for any purpose for which exchange can be purchased from an authorized dealer in India.

k. The Rupay International cards can be used for International transaction at ATM/POS terminals displaying discover dinners club international or pulse logos in contact mode only.

l. The Cardholder is under an obligation not to countermand an order/ Transaction which he/ she has conducted with the Card.

9. Customer Eligibility for Issuance:

a. The Bank may issue VISA & Rupay Brand of Debit cards (Personalized & Non Personalized) to be used at ATM, POS & over the internet for online usage. Cards to be issued after getting customer request in prescribed application form duly filled and signed by the customer.

b. Depending on the business requirement, Bank may however decide for issuance of other brand cards such as Master Card or Amex.

c. Depending on Business requirement, Bank may also explore the possibility of co-branding of debit cards.

d. Bank shall issue Debit Cards to Savings / Current (Individual and Proprietorship) A/c holders and Staff Overdraft Accounts.

e. Bank shall not issue debit cards to cash credit/loan account holders. However, it will not preclude the banks from linking the overdraft facility provided along with Pradhan Mantri Jan Dhan Yojana accounts or Mahabank Kisan Credit Card accounts with a debit card

f. Individual Minor Savings account holders having age 10 & above can be issued Debit Cards under Mahabank Yuva Savings Account Scheme, subject to the safeguards that minor accounts are not allowed to be overdrawn and that these always remain in credit.

g. Personalized Debit Card (Rupay Platinum, VISA) to be issued in Saving & Current (Individuals) account holders.

h. The Debit Card shall be issued with a Welcome kit containing safety tips, usage guidelines as well as terms & conditions detailed in the form of Booklet to avoid any complaints from customer in this regard.

i. Debit Card should not be issued to deceased, inoperative, HUF, Pvt Limited, public limited, Partnership firm, LLP, Club, Society & Association, Trust & to those persons who gives in writing not to avail debit card facility etc.

j. The Bank shall not force a customer to avail debit card facility and shall not link issuance of debit card for availment of any other facility from the bank.

k. Bank shall issue detailed guidelines regarding issuance of Debit Card to pensioners, illiterate and blind persons for branches to have a uniform functionality / implementation across branches.

l. The Bank shall issue Debit card to pensioners, illiterate and blind persons on their request. However, the person applying for debit card should be at least numeric literate and bank employee/s may guide about all the related risks (such as Phishing, Vishing, Card Cloning etc.) to these type of customers at the time of issuance of debit Card.

m. Bank shall provide block / unblock facility of debit card as per requirement of customer.

10. Other Form Factors:

Form Factor is the physical or virtual instrument that can be used in place of a card to undertake a payment/banking transaction.

a. Bank may issue other form factors in place of a plastic debit card such as wearables like smart watches, key chain, payment stickers, bracelet, acrylic watch strap etc. after obtaining explicit consent from the customer.
b. Form factors shall be subject to the specific and general guidelines applicable to respective debit cards.
c. Bank shall provide options for disabling or blocking the form factor in line with the instructions issued by the Reserve Bank from time to time.
d. Detailed report to be submitted to the Department of Regulation, reserve Bank of India, prior to the issuance of any such form factors. If Bank has already issued such product prior to the effective date of the Master Direction, shall submit detailed report to Department of Regulation within 30 days from the effective date.

11. General Conditions:

a. Bank shall keep internal records to enable operations to be traced and errors to be rectified (taking into account the law of limitation for the time barred cases) as prescribed under ‘Master Direction on Know Your Customer’, as amended from time to time.
b. Bank shall provide with a record of the transactions after he/she has completed it, immediately in the form of receipt or another form such as the bank statement/email/SMS.
c. With a view to reducing the instances of misuse of lost/stolen cards, Bank has started issuing EMV enabled Debit Cards to the customers and in future, Bank may consider issuing card with advanced features as per latest technology that may evolve from time to time.
d. Bank has a provision to block a lost card immediately on being informed by the cardholder through Mobile Banking, Internet Banking, WhatsApp Banking Customer care or Branches/offices and formalities, if any, can follow within a reasonable period.
e. Bank has a provision to provide to the cardholder the detailed procedure to report the loss, theft or an unauthorised use of card or PIN. Presently multiple channels such as through branches or offices, customer care, Internet banking, Mobile Banking,

WhatsApp Banking, dedicated e-mail-id, etc. for reporting an unauthorized transaction on 24 x 7 basis and allow the customer to initiate the blocking of the card. The process for blocking the card, should be adequately publicized.

f. Bank has a provision to immediately send a confirmation to the cardholder subsequent to the blocking of a card.

g. Bank shall not dispatch a card to a customer unsolicited. In case of renewal of an existing card, the cardholder shall be provided an option to decline the same if he/she wants to do so before dispatching the renewed card. In case a card is blocked at the request of the customer, replacement card in lieu of the blocked card shall be issued with the explicit consent of the customer. Further, Bank shall obtain explicit consent of the cardholder prior to the renewal of an existing blocked card.

h. Any discounts, cashbacks, reward points, loyalty points or any other benefits offered by the Bank shall be provided in a transparent manner including source of such benefits. The accounting process for the same shall be verifiable in the books of the Bank. Detailed information regarding these benefits shall be displayed on the website of the Bank and a copy of the same shall also be provided to the cardholder.

i. In case of an insurance cover provided with a card, Bank shall ensure that the relevant nomination details are recorded by the Insurance Company and the availability of insurance is included, along with other information, in every statement. The information shall also include the details regarding the insurance cover, name/address and telephone number of the Insurance Company which will handle the claims relating to the insurance cover. For group insurance policies, the information relating to claim process along with the contact details of the concerned official within the bank dealing with the group policy shall be provided in the statements. For Debit cards covered under RuPay Insurance program, Bank should communicate the detailed information, benefits and claim process to Branches/offices/customers.

j. Bank shall issue detailed operational guidelines regarding storage of cards, access to cards, procedure to issue cards and a mechanism to ensure/ reporting of compliances of operational guidelines for minimizing the frauds related to cards (Both Debit Cards and PPI Instruments).

k. In case Bank, at its discretion, decide to block/deactivate/suspend a debit card, it shall be ensured that a standard operating procedure is followed as approved by their Board. Further, it shall also be ensured that blocking/deactivating/suspending a card or withdrawal of benefits available on any card is immediately intimated to the cardholder along with reasons thereof through electronic means (SMS, email, etc.) and other available modes.

12. Terms and conditions for issue of cards to customers:

a. The relationship between the Bank and the cardholder shall be contractual. Bank shall make available to the cardholders in writing, a set of contractual terms and conditions governing the issue and use of such cards. These terms shall be expressed clearly and also maintain a fair balance between the interests of the parties concerned.

b. The terms and conditions for the issue and usage of a card shall be mentioned in clear and simple language (preferably in English, Hindi and the local language) comprehensible to the cardholder.

c. Bank shall not levy any charge that was not explicitly indicated to the cardholder at the time of issue of the card and without getting his/her explicit consent. However, this shall not be applicable to charges which may subsequently be levied by the Government or any other statutory authority. The details of all the existing and revised charges associated with cards shall be displayed on the Bank's website.

d. The convenience fee, if any charged on specific transactions, shall be indicated to the cardholder in a transparent manner, prior to the transaction.

e. The terms shall clearly specify the time-period for reversal of unsuccessful/failed transactions and the compensation payable for failure to meet the specified timeline.

f. The terms may be altered by the Bank, but 30 days' notice of the change shall be given to the cardholder to enable him/her to withdraw if he/she so chooses. After the notice period of 30 days, the cardholder would be deemed to have accepted the terms if he/she had not withdrawn during the specified period. The change in terms shall be notified to the cardholder through all the communication channels available.

g. The terms shall put the cardholder under an obligation to take all appropriate steps to keep the card safe and not to record the PIN or code, in any form that would be intelligible or otherwise accessible to any third party if access is gained to such a record, either honestly or dishonestly.

h. The terms shall specify that the Bank shall exercise care when issuing PINs or codes and shall be under an obligation not to disclose the cardholder's PIN or code to anyone, except to the cardholder.

i. Bank shall issue detailed guidelines regarding issuance of Debit Card to pensioners, illiterate and blind persons and to have a uniform functionality/ implementation across branches.

13. Compliance with Other instructions:

The issue of cards as a payment mechanism is subject to relevant instructions on cash withdrawal, issue of international card, security issues and risk mitigation measures, card-to-card fund transfers, merchant discount rates structure, failed ATM transactions, etc, issued by the Department of Payment and Settlement Systems, Reserve Bank of India under the Payment and Settlement Systems Act, 2007, the Foreign Exchange Department, Reserve Bank of India under Foreign Exchange Management Act, 1999, Master Directions on Digital Payments Security Control, and Bank's guidelines for internal control system and mechanism, with regard to compliance of RBI guidelines, as amended from time to time.

14. Redressal of grievances:

a. Bank shall put in place a Grievance Redressal Mechanism within the card issuing entity and give wide publicity about it through electronic and print media. In-charge Customer Service Department shall ensure that grievances of cardholders are redressed promptly without any delay. Specific timelines may be stipulated in the Board approved policy for issuance of cards, redressal of grievances and compensation framework. The grievance redressal procedure and the Board approved policy shall be displayed on the website of the card-issuer with a clearly visible link on the homepage.

b. Bank shall ensure that the call centre staff are trained adequately to competently handle and escalate, a complaint, if necessary. The Grievance Redressal process shall have a provision for automatic escalation of unresolved complaints from a call center/base level to higher authorities. There shall be a system of acknowledging customers' complaints for follow up, such as complaint number/docket number, even if the complaints are received over phone.

c. Bank shall be liable to compensate the complainant for the loss of his/her time, expenses, financial loss as well as for the harassment and mental anguish suffered by him/her for the fault of the card-issuer and where the grievance has not been redressed in time. If a complainant does not get satisfactory response from the card-issuer **within a maximum period of 30 days** from the date of lodging the complaint, he/she will have the option to approach the Office of the RBI Ombudsman under Integrated Ombudsman Scheme for redressal of his/her grievance/s. Timeline (TAT)

for escalation of complaints, level of escalation and other details pertaining to grievances and compensation shall be governed by Bank's Customer Service Policy.

d. Escalation of Failed ATM Transactions – Bank shall have a proper escalation matrix for resolving the failed ATM transaction complaints within defined TAT.
e. Bank shall follow Customer Grievance Redressal policy for fraud redressal.
f. Bank shall follow Digital Channel Reconciliation Policy – Chapter X for settlement & reconciliation of Debits Cards /POS transactions.

15. Compliance: with Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation under the PMLA, 2002:

The instructions/Directions on KYC/AML/CFT issued by RBI and Bank from time to time, shall be strictly adhered to in respect of all cards issued, including co-branded cards.

16. Hot listing of Debit Card:

Bank must block a lost card immediately on being informed by the customer and formalities, if any, including lodging of FIR by customer in case of theft/fraud can follow within a reasonable period

17. Warm listing of Debit card:

Warm listing is a security feature provided for blocking the debit card on temporary basis. Un-Warm listing is a feature for Un-blocking the debit card of customer that was previously blocked. Bank shall also issue operational guidelines on warm listing of cards.

18. Handling of Customer Complaints/ grievances:

a. Customer should lodge representation/ queries/ complaints, either at the card issuing branch or at the Mahaseva. The card is issued on the condition that the bank bears no liability for unauthorized use of card. The responsibility is fully that of the card holder. Customer shall be aware of any kind of information being shared with any other organization and type of information being shared to avoid any conflicts on part of the Bank.In cases where the loss is due to negligence by a customer, such as where he has shared the authentication 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. Timeline, Grievance redressal procedure, Name, address and contact number of the important executives as well as Grievance redressal officer of the bank etc. for resolution of grievances is given under Bank's Grievance redressal policy. The said information shall be made available on Bank's website and also periodically reviewed/changed.

b. Unsolicited commercial communication: Bank shall ensure that they engage telemarketers who comply with directions/ regulations issued by the Telecom Regulatory Authority of India (TRAI) from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)".

Lost or stolen card reporting by customer:

a. If any Customer's card is lost or stolen or if PIN is disclosed to a third party, customer should report the incident immediately by calling Mahaseva or by sending e-mail to mahaconnect@mahabank.co.in. If customer is travelling overseas, information to be given to the nearest Visa Centre as soon as possible.
b. Customer is liable for all amounts debited to account using Debit Card as a result of the unauthorized use of card/ PIN until reported loss, theft or disclosure of your card or PIN. If the card/PIN, which has been reported lost or stolen, is recovered, it must not be used again.
c. The cardholder should bear the loss sustained up to the time of notification to the bank of any loss, theft or copying of the card. On receipt of notification at bank's customer care/Helpdesk of the loss, theft or copying of the card, the bank will take all action open to it stop within 30 minutes.
d. Customer can hotlist the card, through different channels including hotlisting through Mobile Banking and Internet Banking.

19. Security and Other Aspects:

a. The physical security & safe custody of the Debit card is the sole responsibility of the customer. However, Bank shall ensure system security of the Debit cards.
b. The liability of the customer/ bank is as per the Bank's Compensation policy which is reviewed as per the guidelines of Reserve Bank of India issued time to time.
c. Adherence RBI's master direction on Digital Payment Security Controls vide DoS.C.O.CSITE.SEC.no.1852/31.01.015/2020-21 dt.18.02.2021.

20. Limits, Charges & Features Applicable:

Bank shall issue operational guidelines on revision of debit card limits, charges and features to the employees of the Bank and necessary awareness campaigns shall be conducted for the customers.

a. Insurance cover offered with RUPAY Debit cards is governed by NPCI under RUPAY Insurance program. Bank shall issue guidelines for the Branches after reviewing the directives issued by NPCI from time to time.
b. The Cardholder shall maintain at all times such minimum balance in the Account, as the Bank may stipulate from time to time.
c. The Bank reserves the right at any time to charge the Cardholder for the issue or reissue of a Card and/or any fees/charges for the transactions carried out by the Cardholder on the Card. The fees/charges should be indicated to the cardholder at the time of issue of the card and Bank should get his/her explicit consent. Any government charges, duty or debits, or tax payable as a result of the use of the Card shall be the Cardholder's responsibility and if imposed upon the Bank (either directly or indirectly), the Bank shall debit such charges, duty or tax against the Account.
d. In addition, operators of Shared Networks may impose an additional charge for each use of their ATM/ POS Terminal/other device, and any such charge along with other applicable fees/charges shall be deducted from the Cardholder's Account. There will be separate service charges levied for such facilities as may be announced by the Bank from time to time and deducted from the Cardholder's Account.
e. In the situation that the account does not have sufficient funds to deduct such fees, the Bank reserves the right to deny any further Transactions.
f. In case of accounts classified as overdrawn accounts, the Cardholder will have to rectify the Account balance position immediately. In every such situation where the

Account gets overdrawn, a flat charge could be levied in addition to the interest to be charged on the debit balance in the Account. This charge will be determined by the Bank and will be notified from time to time. In the event of an Account being overdrawn due to Card Transactions, the Bank reserves the right to setoff this amount against any credit lying from any of the Cardholder's other Accounts held jointly or singly without giving any notice. For such accounts, the customers are to be notified before debiting the amount that the amount being debited is an overdraft on which a particular rate of interest will be applied. This will help in reduction of such accounts being turned into NPA in future.

g. Nothing in the Terms shall affect the Bank's right of setoff, transfer and application of monies at law or pursuant to any other agreement from time to time subsisting between the Bank and Cardholder.
h. The Cardholder also authorizes the Bank to deduct from his Account, and indemnifies the Bank against any expenses it may incur in collecting money owed to it by the Cardholder in connection with the Card. (including without limitation reasonable legal fees).
i. The Bank may, at its discretion levy penal charges for non-maintenance of the minimum balance. In addition to the minimum balance stipulation, the Bank may levy service and other charges for use of the Card, which will be notified to the Cardholder from time to time.
j. In the case of transactions entered into by the Cardholder through the internationally valid Debit Card, the equivalent in the currency in which the Cardholder's Account is held, along with processing charges, conversion charges, fees if any charged as per NPCI / VISA regulations, any other service charges for such transactions shall be debited to the Account linked with the Card held at the Bank.
k. The Cardholder authorizes the Bank to recover all charges related to the Card as determined by the Bank from time to time by debiting the Account linked with the Card. Details of the applicable fees and charges as stipulated by the Bank will be displayed on the website and / or at the branches.

21. Fair practices as per BCSBI guidelines for ATM /Debit Cards:

a. Bank will offer customer an ATM / Debit Card if it is normally issued with the type of account customer have opted for.
b. New Cards / Replacement cards (debit as well as credit cards) will be essentially EMV Chip and PIN enabled card only. Customer may decline to accept the card if he/she do not want it.
c. Where cards are delivered to the customers personally, Bank must be satisfied about customer identity before allowing cards to be delivered.
d. Bank will send a service guide / member booklet giving detailed terms and conditions, losses on customer account that the customer may be liable if the card is lost / misused, and other relevant information with respect to usage of card, along with the first card.
e. Bank will inform customer which of his/her accounts the card can access. Bank will also inform customer whether the card issued to him/her has more than one function and if so, what those functions are.
f. Bank will advise customer of the current transaction limits that apply at POS counters, ATMs and forex transactions.
g. Bank will advise customer of the fees and charges that apply to his/her card.
h. Customer shall safeguard his/her card by taking the following measures:

    i. Sign the card as soon as you receive it.

ii. Do not leave the card unattended (in a wallet / purse) or in a location (e.g. vehicle) from where it could be removed without being noticed
iii. Do not give the card to anyone or let anyone else use the card including at merchant establishments (e.g. restaurants, petrol pump, etc.)
iv. Always remember to take the card back after using it.
v. Inform the bank if customer changes his/her address with documentary proof so that, whenever required, a replacement card is sent to correct address.
vi. Complaints relating to disputed / failed ATM transactions are to be lodged with card issuing bank (through-authorized officials or channel).

22. Co-branding arrangement:

Co-branded Card is a card that is issued jointly by a card-issuer and a co-branding entity bearing the names of both the partnering entities.

The co-branding arrangement shall be as per the Bank's Board approved policy. The policy shall specifically address issues pertaining to various risks, including reputation risk associated with such an arrangement and put in place suitable risk mitigation measures.

Bank, which were granted specific approvals for issue of co-branded debit cards in the past, are advised to ensure that the co-branding arrangement is in conformity with the instructions issued under IT Procurement Policy. In case, the co-branding arrangement is between two banks, the card issuing bank shall ensure compliance with the relevant instructions.

23. Issue of Co-Branded Cards:

a. Prior approval of the Reserve Bank is not necessary for the issuance of co-branded debit cards/co-branded prepaid cards by banks and co-branded credit cards by Bank subject to conditions stipulated under this policy. However, UCBs shall not issue debit/credit cards in tie-up with other non-bank entities. In addition to the conditions listed herein, the co-branding arrangement for credit cards, debit cards and prepaid cards shall also be subject to the specific conditions applicable to such cards.
b. The co-branded credit/debit card shall explicitly indicate that the card has been issued under a co-branding arrangement. The co-branding partner shall not advertise/market the co-branded card as its own product. In all marketing/advertising material, the name of the Bank shall be clearly shown.
c. The co-branded card shall prominently bear the branding of the Bank.

24. Due diligence:

Bank shall carry out due diligence in respect of the co-branding partner entity with which they intend to enter into tie-up for issue of such cards to protect themselves against the reputation risk they are exposed to in such an arrangement. Bank shall ensure that in cases where the proposed co-branding partner is a financial entity, it has obtained necessary approvals from its regulator for entering into the co-branding arrangement.

25. Outsourcing of activities:

Bank shall also be liable for the acts of the co-branding partner. The card-issuer shall ensure adherence to the guidelines on 'Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks', as amended from time to time. Bank shall ensure that cash backs, discounts and other offers advertised by a co-branding partner

are delivered to the cardholder on time. Bank shall be liable for any delay or non-delivery of the same to the cardholders. Outsourcing of activities shall be as per the Bank's Outsourcing Policy issued time to time.

26. Role of co-branding partner entity:

a. The role of the co-branding partner entity under the tie-up arrangement shall be limited to marketing/distribution of the cards and providing access to the cardholder for the goods/services that are offered.

27. Review of operations:

The ORMC Committee shall undertake review of operations/issue of debit cards on half-yearly basis. The review shall include, inter-alia, card usage analysis including cards not used for long durations and the inherent risk therein.

28. Standard Operating Procedure:

Bank shall issue comprehensive SOP for Issuance of Debit cards, Card renewal on expiry, Issuance of duplicate debit cards, debit card limits, debit card features, debit card charges, handling of debit cards, handling of customer complaints/grievances etc. and FAQs from time to time.

29. Confidentiality of Customer Information

(a) Bank shall not reveal any information relating to customers obtained at the time of opening the account or issuing the card to any other person or organization without obtaining their explicit consent, with regard to the purpose/s for which the information will be used and the organizations with whom the information will be shared. Bank shall ensure strict compliance to the extant legal framework on data protection. Further, in case where the customers give explicit consent for sharing the information provided by them with other agencies, Bank shall clearly state and explain to the customer the full meaning/implications of the disclosure clause. The information sought from customers shall not be of such nature which will violate the provisions of law relating to maintenance of secrecy in the transactions. The Bank shall be solely responsible for the correctness or otherwise of the data provided for the purpose.

(b) Bank shall ensure that the co-branding arrangement is in conformity with the instructions issued for co-branding by RBI. In case, the co-branding arrangement is between two banks, the card issuing bank shall ensure compliance with the relevant instructions.

30. Outsourcing of Various Services:

Bank shall ensure adherence to the master directions on 'Outsourcing of Information Technology Services' and guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services, as amended from time to time. Further, the Bank shall not share card data (including transaction data) of the cardholders with the outsourcing partners unless sharing of such data is essential to discharge the functions assigned to the latter. In case of sharing of any data as stated above, explicit consent from the cardholder shall be obtained. It shall also be ensured that the storage and the ownership of card data remains with the Bank.

31. References:

a. Bank circular no. AX1/IT/IT/199/382/2018-19 dated 03.09.2018 on Cash @ POS at Merchant Establishment.
b. RBI circular no. DPSS.CO.PD.No.449/02.14.003/2015-16 dated 27/08/2015 on cash withdrawal @ POS.
c. AX1/PLN/KYC-AML-CFT/Cir.No.10 /2018-19 dated 02.08.2018
d. Bank Grievance Redressal policy.
e. RBI Circular No. RBI/2017-18/4 FIDD.CO.FSD.BC.No.7/05.05.010/2017-18 dated 03.07.2017
f. RBI Circular No. RBI/2022-23/92 DoR.AUT.REC.No.27/24.01.041/2022-23 dated 21.04.2022
g. DoS.C.O.CSITE.SEC.no.1852/31.01.015/2020-21 dt.18.02.2021
h. Amendment to the Master Direction - Credit Card and Debit Card – Issuance and Conduct Directions, 2022 dated 07.03.2024
i. Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions dated 06.07.2017

Chapter- II

PPI Issuance and Operations

1. Preamble:

One of the functions of the Bank is to issue Pre Paid Instruments (PPI) and its all variants to customer through its large network of branches across India. In order to encourage banks issuance and operations of PPI, RBI has issued Master Directions on Prepaid Payment Instruments (PPIs), RBI/DPSS/2021-22/82 CO.DPSS.POLC.No.S-479/02.14.006/2021-22 dated 27th August 2021, updated on 12th November 2021, and asked for formulation of Bank's own Board approved PPIs issuance and operations policy.

The RBI has issued a number of circulars from time to time on issuance and operations of PPIs. In light of developments in the field, progress made by PPI issuers, experience gained and with a view of foster innovation and competition, ensure safety and security, customer protection, etc.

2. Purpose:

To start issuance of PPIs to customers as per the RBI's framework for authorization, regulation and supervision of entities.

This policy document on PPI Issuance and Operations outlines the guiding principles in respect of issuance of Small PPIs and Full-KYC PPIs payment instruments, types of permitted transactions, discounting, settlement and dispute resolution in Bank of Maharashtra.

This policy will apply to all the three types of PPIs issuance and operations on various digital platforms initiated by the Bank. The policy will be guided by Payment & Settlement systems act 2007.

3. Definitions:

a. **Issuer:** Entities operating the payment systems issuing PPIs to individuals/organizations. The money so collected is used by these entities to make payment to the merchants who are part of the acceptance arrangement and for facilitating funds transfer/remittance services.

b. **PPI holder**: Individuals / Organizations who obtain/purchase PPIs from the issuers and use the same for purchase of goods and services, including financial services, remittance facilities, etc.

c. **Prepaid Payment Instruments (PPIs):** PPIs are payment instruments that facilitate purchase of goods and services, including financial services, remittance facilities, etc., against the value stored on such instruments. The PPIs that require RBI approval /authorization prior to issuance are classified under two types vis. (i) Small PPIs, and (ii) Full-KYC PPIs.

   i. **Small PPIs :** Issued by banks and non-banks after obtaining minimum details of the PPI holder. They shall be used only for purchase of goods and services. Funds transfer or cash withdrawal from such PPIs shall not be permitted. Small PPIs can be used at a group of clearly identified merchant locations / establishments which have a specific contract with the issuer (or contract through a payment aggregator / payment

ii. **Full-KYC PPIs :** Issued by banks and non-banks after completing Know Your Customer (KYC) of the PPI holder. These PPIs shall be used for purchase of goods and services, funds transfer or cash withdrawal.

d. **Limits:** All 'limits' in the value of instruments stated in the policy, indicate the maximum value of such instruments, denominated in INR, that shall be issued to any holder, unless otherwise specified.

e. **Holder:** Individuals / Organisations who obtain / purchase PPIs from the issuer and use them for purchase of goods and services, financial services, remittance facilities, etc.

f. **Issuer:** Entities issuing PPIs to individuals / organisations.

g. **Merchants**: These are establishments who have a specific contract to accept the PPIs issued by the PPI issuer (or contract through a payment aggregator / payment gateway) against the sale of goods and services, including financial services.

h. **Net-worth:** Net-worth will consist of 'paid up equity capital, preference shares which are compulsorily convertible into equity capital, free reserves, balance in share premium account reserves representing surplus arising out of sale proceeds of assets but not reserves created by revaluation of assets' adjusted for 'accumulated loss balance, book value of intangible assets and deferred revenue expenditure, if any'.

i. **Acquirer:** The bank that provides necessary infrastructure to the merchant to accept payment, maintain relationship and facilitate acceptance of payments through cards/ digital channels.

j. **Intermediary Agency:** Agencies who facilitate interbank settlements.

k. **PPI Issuing Bank:** Bank which issues the PPIs

l. **Regulator:** RBI regulates the electronic payments in India.

4. Eligibility requirements for issuance of PPIs by banks:

In accordance with RBI guidelines, Bank shall issue PPIs only after obtaining approval from RBI.

5. Safeguards against Money Laundering (KYC / AML / CFT) Provisions:

a. The Know Your Customer (KYC) / Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) guidelines issued by the Department of Banking Regulation (DBR), RBI, in their "Master Direction – Know Your Customer (KYC) Directions, 2016" updated from time to time, shall apply mutatis mutandis to Bank and its agents.

b. As PPI are operating a Payment System, provisions of Prevention of Money Laundering Act, 2002 (PMLA) and Rules framed thereunder, as amended from time to time, are also applicable.

c. Bank shall maintain a log of all the transactions undertaken using the PPIs for at least ten years. This data shall be made available for scrutiny to RBI or any other agency / agencies as may be advised by RBI. Bank shall also file Suspicious Transaction Reports (STRs) to Financial Intelligence Unit-India (FIU-IND). The Bank shall monitor

& review the performance of Authorised/designated agents anually, review of security measures through transaction logs.

6. Issuance, loading and reloading of PPIs:

a. RBI has permitted Bank to issue reloadable or non – reloadable PPIs depending upon the permissible type / category of PPIs.

b. Bank shall ensure that the name of the company which has received approval/ authorisation for issuance and operating of PPIs, is prominently displayed along with the PPI brand name in all instances. Bank shall also regularly keep RBI informed regarding the brand names employed / to be employed for their products.

c. Bank shall ensure that no interest is payable on PPI balances. Bank shall maintain a log of all the transactions undertaken using the PPIs for at least ten years. This data shall be made available for scrutiny to RBI or any other agency / agencies as may be advised by RBI. The PPI issuers shall also file Suspicious Transaction Reports (STRs) to Financial Intelligence Unit-India (FIU-IND).

d. PPIs shall be permitted to be loaded / reloaded by cash, by debit to a bank account, by credit and debit cards, PPIs (as permitted from time to time) and other payment instruments. The electronic loading / reloading of PPIs shall be through above payment instruments issued only by regulated entities in India and shall be in INR only.

e. Cash loading to PPIs shall be limited to Rs.50,000/- per month subject to overall limit of the PPI.

f. The PPIs may be issued as cards, wallets, and any such form / instrument which can be used to access the PPI and to use the amount therein. PPIs in the form of paper vouchers shall not be issued.

g. Bank shall issue and reload PPIs at branches, ATMs and through the BCs appointed as per the guidelines issued by RBI in this regard.

h. Bank shall issue and reload PPIs through their authorised outlets or through authorised / designated agents subject to following conditions:

   i. Bank shall carry out proper due diligence of the persons appointed as authorised / designated agents for issue / reloading of permissible categories of PPIs.
   ii. Bank shall be responsible as the principal for all acts of omission or commission of their authorised / designated agents, including safety and security aspects.
   iii. Bank shall ensure preservation of records and confidentiality of customer information in it's own possession as well as in the possession of it' authorised / designated agents.
   iv. Bank shall regularly monitor the activities of authorised / designated agents and also carry out a review of the performance of various agents engaged, at least once in a year.
   v. Bank and its authorised / designated agents shall ensure adherence to applicable laws of the land, including KYC / AML / CFT norms as indicated in paragraph. 6.

j. Bank shall ensure that there is no co-mingling of funds originating from any other activity that the Bank may be undertaking such as BCs of bank/s, intermediary for payment aggregation, payment gateway facility, etc.

k. PPIs under co-branding arrangements:

i. The co-branding partner shall be a company incorporated in India and registered under the Companies Act 1956 / Companies Act 2013. The co-branding partner can also be a Government department / ministry. In case the co-branding partner is a bank, then the same shall be a bank licensed by RBI.

ii. Bank shall carry out due diligence in respect of the co-branding partner to protect against the reputation risk. In case of proposed tie up with a financial entity, Bank may ensure that entity has the approval of its regulator for entering into such arrangement.

iii. The instructions / guidelines on KYC / AML / CFT (as indicated in paragraph 6) shall be adhered to, in respect of all PPIs issued under the co-branding arrangement as well.

iv. Bank shall be liable for all acts of the co-branding partner. Bank shall also be responsible for all customer related aspects of the PPIs.

v. Bank shall be permitted to co-brand such instruments with the name / logo of the company for whose customers / beneficiaries such co-branded instruments are to be issued.

vi. The name of Bank shall be prominently visible on the payment instrument.

vii. In case of co-branding arrangements between bank and non-bank entity, the bank shall be the PPI Issuer. The role of the non-bank entity shall be limited to marketing / distribution of the PPIs or providing access to the PPI holder to the services that are offered.

viii. In case of co-branding arrangement between two banks, then the PPI issuing bank shall ensure compliance to above instructions.

l. There shall be no remittance without compliance to KYC requirements.Bank including its agents, shall not create new PPIs each time for facilatating cash-based remittance to other PPIs / bank accounts. PPIs created for previous remittance by the same person shall be used.

7. Cross-Border Transactions:

The use of INR denominated PPIs for cross border transactions shall not be permitted except as under:

a. **PPIs for cross-border outward transactions**

i. KYC compliant reloadable Small PPIs and Full-KYC PPIs issued by bank shall be permitted to be used in cross-border outward transactions (only for permissible current account transactions under FEMA viz. purchase of goods and services), subject to adherence to extant norms governing such transactions.

ii. PPIs shall not be used for any cross-border outward fund transfer and/or for making remittances under the Liberalised Remittance Scheme. Prefunding of online merchant's account shall not be permitted using such Rupee denominated PPIs.

iii. Bank shall enable the facility of cross-border outward transactions only on explicit request of the PPI holders and shall apply a per transaction limit not exceeding Rs.10,000/-, while per month limit shall not exceed Rs. 50,000/- for such cross- border transactions.

iv. In case this facility is made available by issuing the PPI in card form, then this PPI shall be EMV Chip and PIN compliant.

v. Such PPIs need not be issued as a separate category of PPI.

b. **PPIs for credit towards cross-border inward remittance**

i. Bank, if appointed as the Indian agent of the authorised overseas principal, can issue PPIs to beneficiaries of inward remittance under the Money Transfer Service Scheme (MTSS) of the RBI.

ii. The PPIs shall be KYC compliant, reloadable and issued only in electronic form, including cards.

iii. Such PPIs shall be issued in adherence to extant norms under the MTSS Guidelines issued by Foreign Exchange Department, RBI.

iv. Amounts only upto Rs.50,000/- from individual inward MTSS remittance shall be permitted to be loaded / reloaded in full-KYC PPIs issued to beneficiaries. Amount in excess of Rs.50,000/- under MTSS shall be paid by credit to a bank account of the beneficiary. Full details of the transactions shall be maintained on record for scrutiny.

v. The roles and responsibilities of the Bank for the PPI related activities shall be distinct from the roles and responsibilities as Indian Agents under MTSS.

vi. Such PPIs need not be issued as a separate category of PPI.

8. Types of PPIs:

a. Small PPIs (or Minimum-detail PPIs)

i. **PPIs upto Rs.10,000/- (with cash loading facility)**

a) Bank can issue such PPIs after obtaining minimum details of the PPI holder;
b) Minimum details shall necessarily include a mobile number verified with One Time Password (OTP) and a self-declaration of name and unique identity / identification number of any 'mandatory document' or 'Officially Valid Document (OVD)' or any such document with any name listed for this purpose in the Master Direction on KYC, as amended from time to time;
c) Such PPIs shall be reloadable in nature;
d) Amount loaded in such PPIs during any month shall not exceed Rs.10,000/- and the total amount loaded during the financial year shall not exceed Rs.1,20,000/
e) Amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000/-;
f) Total amount debited from such PPIs during any month shall not exceed Rs.10,000/;
g) These PPIs shall be used only for purchase of goods and services. Cash withdrawal or funds transfer from such PPIs shall not be permitted;
h) There shall be no separate limit for purchase of goods and services using PPIs; Bank may decide limit for these purposes within the overall PPI limit;
i) These PPIs shall be converted into full-KYC PPIs within a period of 24 months from the date of issue of the PPI, failing which no further credit shall be allowed in such PPIs. However, the PPI holder shall be allowed to use the balance available in the PPI;
j) This category of PPI shall not be issued to the same user in future using the same mobile number and same minimum details;
k) Bank shall give an option to close the PPI at any time. The closure proceeds can be transferred 'back to source account' (payment source from where the

PPI was loaded). Alternatively, the closure proceeds can be transferred to a bank account after complying with KYC requirements of PPI holder; and

l) The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.

ii. **PPIs upto Rs.10,000/- (with no cash loading facility)**

a) Banks can issue such PPIs after obtaining minimum details of the PPI holder;
b) Minimum details shall necessarily include a mobile number verified with OTP and a self-declaration of name and unique identity / identification number of any 'mandatory document' or OVD or any such document with any name listed for this purpose in the Master Direction on KYC, as amended from time to time;
c) Such PPIs shall be reloadable in nature. Loading / Reloading shall be from a bank account / credit card / full-KYC PPI;
d) The amount loaded in such PPIs during any month shall not exceed Rs.10,000 and the total amount loaded during the financial year shall not exceed Rs.1,20,000;
e) The amount outstanding at any point of time in such PPIs shall not exceed Rs.10,000;
f) These PPIs shall be used only for purchase of goods and services. Cash withdrawal or funds transfer from such PPIs shall not be permitted;
g) Bank shall give an option to close the PPI at any time. The closure proceeds can be transferred 'back to source account' (payment source from where the PPI was loaded). Alternatively, the closure proceeds can be transferred to a bank account after complying with KYC requirements of PPI holder;
h) The features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds; and
i) The PPIs of paragraph 9.1 (i) existing as on December 24, 2019 can be converted to this type of PPI, if desired by the PPI holder.

b. Full-KYC PPIs

i. Bank can issue such PPIs after completing KYC of the PPI holder (as indicated in paragraph 6);
ii. The Video-based Customer Identification Process (V-CIP), as detailed in Department of Regulation's Master Direction on KYC dated February 25, 2016 (as amended from time to time), can be used to open full-KYC PPIs as well as to convert Small PPIs of paragraph 9.1 into full-KYC PPIs;
iii. Such PPIs shall be reloadable in nature;
iv. The amount outstanding shall not exceed Rs.2,00,000/- at any point of time;
v. The funds can be transferred 'back to source account' (payment source from where the PPI was loaded) or 'own bank account of the PPI holder' (duly verified by the PPI issuer). However, Bank shall set the limits considering the risk profile of the PPI holders, other operational risks, etc.;
vi. Bank shall provide the facility of 'pre-registered beneficiaries' whereby the PPI holder can register the beneficiaries by providing their bank account details, details of PPIs issued by same issuer (or different issuer as and when permitted), etc.;

vii. In case of such pre-registered beneficiaries, the funds transfer limit shall not exceed Rs.2,00,000/- per month per beneficiary. Bank shall set the limits within this ceiling considering the risk profile of the PPI holders, other operational risks, etc. PPI issuer shall set the limits within this ceiling considering the risk profile of the PPI holder, other operational risk etc.

viii. Funds transfer limits for all other cases shall be restricted to Rs.10,000/- per month;

ix. Funds transfer from such PPIs shall also be permitted to other PPIs, debit cards and credit cards as per the limits given above;

x. There is no separate limit on purchase of goods and services using PPIs and Bank may decide limit for these purposes within the overall PPI limit;

xi. Bank shall clearly indicate these limits to the PPI holders and provide necessary options to PPI holders to set their own fund transfer limits;

xii. Bank shall also give an option to close the PPI and transfer the balance as per the applicable limits of this type of PPI. For this purpose, the issuer shall provide an option, including at the time of issuing the PPI, to the holder to provide details of pre-designated bank account or other PPIs of the bank (or other issuer as and when permitted) to which the balance amount available in the PPI shall be transferred in the event of closure of PPI, expiry of validity period of such PPIs, etc.;

xiii. Cash withdrawal at PoS devices shall be subjected to a limit of Rs.2,000/- per transaction within an overall monthly limit of Rs.10,000/- across all locations (Tier 1 to 6 centres), subject to conditions stipulated in RBI circular DPSS.CO.PD.No.449/02.14.003/2015-16 dated August 27, 2015;

xiv. Features of such PPIs shall be clearly communicated to the PPI holder by SMS / e-mail / any other means at the time of issuance of the PPI / before the first loading of funds.

c. Specific categories of PPIs:

Gift PPIs

Bank shall issue prepaid gift instruments subject to the following conditions:

i. Maximum value of each prepaid gift instrument shall not exceed Rs.10,000/-

ii. These instruments shall not be reloadable.

iii. Cash-out or refund or funds transfer shall not be permitted for such instruments.

iv. KYC (as indicated in paragraph 6) details of the purchasers of such instruments shall be maintained by the Bank. Separate KYC would not be required for customers who are issued such instruments against debit to their bank accounts and / or credit cards in India.

v. Bank shall adopt a risk based approach, duly approved by their Board, in deciding the number of such instruments which can be issued to a customer, transaction limits, etc.

vi. The gift instruments may be revalidated (including through issuance of new instrument) as and when requested by the PPI holder.

vii. The features of such PPIs shall be clearly communicated to the PPI holder by SMS/e-mail / post or by any other means at the time of issuance of the PPI / before the first loading of funds.

PPIs for Mass Transit Systems (PPI-MTS)

Bank would issue Mass Transit Systems –PPIs instruments subject to the following conditions:

i. These PPIs shall contain the Automated Fare Collection application related to transit services, toll collection and parking.
ii. Such PPIs shall be enabled only for payments across various modes of public transport such as metro, buses, rail, & waterways, tolls and parking.
iii. These PPIs can be issued without KYC verification of the holders.
iv. These PPI can be reloadable in nature.
v. The amount outstanding, in such PPIs shall not exceed Rs.3,000/- at any point of time.
vi. These PPIs can have perpetual validity.
vii. Cash-withdrawal, refund or funds transfer shall not be permitted in such PPIs.

PPIs to Foreign Nationals / Non-Resident Indians (NRIs) visiting India

i. PPIs can be issued in INR denominated full-KYC PPIs to foreign nationals / NRIs visiting India (to start with, this facility will be extended to travelers from the G-20 countries, arriving at select international airports). Such PPIs can also be issued in co-branding arrangement with entities authorized to deal in Foreign Exchange under FEMA.
ii. The PPIs shall be issued after physical verification of Passport and Visa of the customers at the point of issuance. Bank shall ensure that such information and record thereof are maintained.
iii. The PPIs can be issued in the form of wallets linked to UPI and can be used for merchant payments (P2M) only;
iv. Loading / Reloading of such PPIs shall be against receipt of foreign exchange by cash or through any payment instrument.
v. The conversion to Indian Rupee shall be carried out only by entities authorised to deal in Foreign Exchange under FEMA.
vi. The amount outstanding at any point of time in such PPIs shall not exceed the limit applicable on full-KYC PPIs.
vii. Provisions of paragraph 14 on validity and redemption, as applicable, shall be adhered to. The unutilized balances in such PPIs can be encashed in foreign currency or transferred ‘back to source’ (payment source from where the PPI was loaded), in compliance with foreign exchange regulations

9. Settlement and Reconciliation:

Settlement and reconciliation procedure shall be followed for all the transactions carried out through Pre-paid payment Instruments.

The settlement shall be carried out as per RBI directives on Harmonization of Turn Around Time (TAT) and customer compensation for failed transactions. The required transaction data logs from various entities including ATM Switch, intermediary, core banking etc. should be obtained and processed.

As per the circular, RBI issued guidelines regarding TAT to be followed by banks for reversal of failed transactions to the account of customers. In case of delay in crediting to

customer, bank will have to pay an additional compensation of Rs100 per day from the TAT date. Bank shall follow TAT and compensation guidelines issued by regulator time-to-time.

The 'Digital Channel Reconciliation Department' is entrusted with the responsibility of ensuring periodic reconciliation of transactions, carried out through various mode of card / cardless electronic platform. Status of reconciliation of transactions to be placed to General Manager/Dy. General Manager DBD on Quarterly Basis

10. Interoperability:

a. Interoperability is the technical compatibility that enables a payment system to be used in conjunction with other payment systems.

b. Bank shall be guided by the technical specifications / standards / requirements for achieving interoperability through UPI and card networks as per the requirements of National Payments Corporation of India (NPCI) and the respective card networks.

c. Bank shall have a Board approved policy for achieving PPI interoperability.

d. Requirements for achieving interoperability: Common to wallets and cards:

   i. Where PPIs are issued in the form of wallets, interoperability across PPIs shall be enabled through UPI.

   ii. Where PPIs are issued in the form of cards (physical or virtual), the cards shall be affiliated to the authorised card networks.

   iii. PPI-MTS shall remain exempted from interoperability, while Gift PPI issuer (both banks and non-banks) have the option to offer interoperability.

   iv. The interoperability shall be facilitated to all KYC-compliant PPIs and entire acceptance infrastructure. It shall be mandatory for Bank to give the holders of full-KYC PPIs (KYC-compliant PPIs) interoperability through authorized card networks (for PPIs in the form of cards) and UPI (for PPIs in the form of wallets).

   v. Interoperability shall be mandatory on the acceptance side as well. QR codes in all modes shall be interoperable by March 31, 2022 vide RBI circular DPSS.CO.PD.No.497/ 02.14.003/2020-21 dated October 22, 2020. For other modes of acceptance, as also for issuance, the interoperability shall be achieved by March 31, 2022. Once a non-bank PPI entity becomes interoperable (on both issuing and acquiring side simultaneously), the entire merchant base, including those acquired by the banks, shall be accessible through the card networks and UPI.

   vi. Technical requirements: Bank shall adhere to all the requirements of card networks / UPI including membership type and criteria, merchant on-boarding, adherence to various standards, rules and regulations applicable to the specific payment system such as technical requirements, certifications and audit requirements, governance, etc.

   vii. Reconciliation, customer protection and grievance redressal :

      a) Bank shall ensure adherence to all guidelines / requirements of card networks / UPI in terms of reconciliation of positions at daily / weekly / monthly or more frequent basis, as the case may be.
      b) Bank shall adhere to all dispute resolution and customer grievance redressal mechanisms as prescribed by the card networks / NPCI.

e. Requirements for achieving interoperability through card networks

i. Card networks are allowed to onboard PPI issuer to join their network. Non-bank PPI issuer is permitted to participate as member / associate member of authorized card networks.

ii. Settlement: For the purpose of settlement, a non-bank PPI issuer can participate directly or through a sponsor bank arrangement as the case may be. Non-bank PPI issuer shall adhere to the requirements of respective card network's settlement system.

iii. Safety and security:

a) Banks and non-banks shall ensure that all new PPIs issued in the form of cards are EMV Chip and PIN compliant.
b) Banks and non-banks shall ensure that all reissuance / renewal of PPIs in the form of cards are EMV Chip and PIN compliant.
c) Gift PPIs may continue to be issued with or without EMV Chip and PIN enablement.

f. Requirements for achieving interoperability through UPI

i. Bank shall facilitate all basic / standard features of interoperability of UPI.

ii. Bank shall act as Payment System Providers (PSP) in UPI.

iii. Bank as PSP shall not on-board customers of any bank or any other PPI issuer.

iv. Authentication shall be completed by the PPI holder as per her / his existing wallet credentials. In other words, a transaction will be pre-approved before it reaches the UPI.

11. Deployment of money collected:

For the schemes operated by banks, the outstanding balance shall be part of the 'net demand and time liabilities' for the purpose of maintenance of reserve requirements. This position will be computed on the basis of balances appearing in the books of the bank as on the date of reporting.

12. Validity and Redemption:

a. All PPIs issued shall have a minimum validity period of one year from the date of last loading / reloading in the PPI. Bank shall issue PPIs with a longer validity. In case the PPI is issued in the form of card (with validity period mentioned on the card, maximum validity of 5 years), then the customer shall have the option to seek replacement of the card.

b. Bank shall caution the PPI holder at reasonable intervals, during the 45 days' period prior to expiry of the validity period of the PPI. The caution advice shall be sent by SMS/ e-mail / post or by any other means in the language preferred by the holder indicated at the time of issuance of the PPI.

c. Banks issuing PPIs shall be guided by the instructions on Depositor Education and Awareness Fund issued by Department of Banking Regulation, RBI, vide, circular DBOD.No.DEAF Cell.BC.101/30.01.002/2013-14 dated March 21, 2014, as amended from time to time.

d. Bank shall clearly indicate the expiry period of the PPI to the customer at the time of issuance of PPIs. Such information shall be clearly enunciated in the terms and conditions of sale of PPI. Where applicable, it shall also be clearly outlined on the website / mobile application of the Bank.

e. PPIs with no financial transaction for a consecutive period of one year shall be made inactive by Bank after sending a notice to the PPI holder/s. These can be reactivated only after validation and applicable due diligence i.e. confirmation of Identify the customer/s who has approached the Branch for reactivating PPI, obtain latest KYC documents of PPI holder/s and verify the same from originals. These PPIs shall be reported to RBI separately.

f. The holders of PPIs shall be permitted to redeem the outstanding balance in the PPI, if for any reason the scheme is being wound-up or is directed by RBI to be discontinued.

13. Transactions Limits:

a. The holder is allowed to use the PPI for these purposes within the overall PPI limit applicable. Bank shall decide to put in place such limits taking into account the risk perception of the holders as per the risk management policy.

b. All financial limits indicated against each type / category of the PPI shall be strictly adhered.

c. Handling refunds:

i. Refunds in case of failed / returned / rejected / cancelled transactions shall be applied to the respective PPI immediately, to the extent that payment was made initially by debit to the PPI, even if such application of funds results in exceeding the limits prescribed for that type / category of PPI.

ii. However, refunds in case of failed / returned / rejected / cancelled transactions using any other payment instrument shall not be credited to PPI.

iii. Bank shall be required to maintain complete details of such returns / refunds, etc., and be in readiness to provide them as and when called for.

Further, Bank shall also put in place necessary systems that enables it to monitor frequent instances of refunds taking in place in specific PPIs and be in a position to substantiate with proof for audit / scrutiny purposes.

14. Security, Fraud prevention and Risk Management Framework:

a. A strong risk management system is necessary for Bank to meet challenges of fraud and ensure customer protection. Bank shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.

b. To meet the challenges of fraud and ensure customer protection. Bank shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.

c. Bank shall inclide all PPI products in Information Security policy for the safety and security of the payment systems operated by them, and implement security measures in accordance with this policy to mitigate identified risks. Bank shall review the security measures

i. on on-going basis but at least once a year,
ii. after any security incident or breach, and
iii. before / after a major change to their infrastructure or procedures.

d. Bank shall ensure that the following framework is put in place to address the safety and security concerns, and for risk mitigation and fraud prevention:

i. In case of wallets, Bank shall ensure that if same login is provided for the PPI and other services offered by the Bank, then the same shall be clearly informed to the customer by SMS or email or post or by any other means. The option to logout from the website / mobile account shall be provided prominently.

ii. Bank shall put in place appropriate mechanisms to restrict multiple invalid attempts to login / access to the PPI, inactivity, timeout features, etc.

iii. Bank shall introduce a system where every debit transactions in wallet is authenticated by explicit customer consent after validation through a Two Factor Authentication (2FA).

iv. Cards (physical or virtual) shall necessarily have Additional Factor of Authentication (AFA) as required for debit cards.

v. 2FA / AFA is not mandatory for PPIs issued under PPI-MTS and gift PPIs.

vi. The transactions undertaken using PPIs through National Electronic Toll Collection (NETC) system can be performed as per the instructions given in DPSS circular DPSS.CO.PD.No.1227/02.31.001/2019-20 dated December 30, 2019, as amended from time to time.

vii. Processing of e-mandate for transactions undertaken using PPIs (cards and wallets) shall be performed, as per the instructions contained in DPSS circular DPSS.CO.PD.No. 447/02.14.003/2019-20 dated August 21, 2019, as amended from time to time.

viii. Bank shall provide customer induced options for fixing a cap on number of transactions and transaction value for different types of transactions / beneficiaries. Customers shall be allowed to change the caps, with additional authentication and validation.

ix. Bank shall put in place a limit on the number of beneficiaries that may be added in a day per PPI.

x. Bank shall introduce a system of alert when a beneficiary is added.

xi. Cooling period of 4hrs for funds transfer upon opening the PPI or loading / reloading of funds into the PPI or after adding a beneficiary so as to mitigate the fraudulent use of PPIs.

xii. Bank shall put in place a mechanism to send alerts when transactions are done using the PPIs. In addition to the debit or credit amount intimation, the alert shall also indicate the balance available / remaining in the PPI after completion of the said transaction. For transactions undertaken in offline mode, as allowed from time to time, the transaction alert shall be sent as soon as the details of transaction are received by the Bank. There is no compulsion to send separate alert for each transaction; however, details of each transaction shall be adequately conveyed as soon as such information reaches the Bank.

xiii. Bank shall put in place mechanism for velocity check on the number of transactions effected in a PPI per day / per beneficiary.

xiv. Bank shall also put in place suitable mechanism to prevent, detect and restrict occurrence of fraudulent transactions including loading / reloading funds into the PPI.

xv. Bank shall put in place suitable internal and external escalation mechanisms in case of suspicious operations, besides alerting the customer in case of such transactions.

e. Bank shall put in place centralised database / management information system (MIS) to prevent multiple purchase of PPIs at different locations, leading to circumvention of limits, if any, prescribed for the issuance. In case of full-KYC PPIs issued by scheduled commercial banks for government departments, the limit of Rs.2,00,000/- shall be for each PPI, provided the PPIs are issued for expenses of the concerned government department and the loading is from the bank account of the government department.

f. Where direct interface is provided to their authorised / designated agents, Bank shall ensure that the compliance to regulatory requirements is strictly adhered to by these systems also.

g. Bank shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. Any such incident should be reported to CISO for onwards submission to RBI/Cert-IN. The same shall be reported immediately to DPSS, RBI, Central Office, Mumbai. It shall also be reported to CERT-IN as per the details notified by CERT-IN.

h. PPI issuer shall also be guided by the following circulars:

   i. DPSS.CO.PD No.1343/02.14.003/2019-20 dated January 15, 2020 (as amended from time to time) on 'Enhancing Security of Card Transactions'. This circular, *inter alia*, gives the facility to card holders to switch on / off and set / modify the transaction limits across multiple channels.
   ii. DPSS.CO.OD.No.1934/06.08.005/2019-20 dated June 22, 2020 (as amended from time to time) on Increasing Instances of Payment Frauds – Enhancing Public Awareness Campaigns Through Multiple Channels.
   iii. CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 dated August 03, 2021 (as amended from time to time) on Framework for Outsourcing of Payment and Settlement-related Activities by PSOs. The bank PPI issuer shall be guided by the outsourcing related instructions issued by their regulatory and supervisory departments.
   iv. The bank PPI issuer shall be guided by the Bank's Outsourcing Policy.

15. <u>Customer Protection and Grievance Redressal Framework:</u>

a. Bank shall disclose all important terms and conditions in clear and simple language (preferably in English, Hindi and the local language) to the holders while issuing the instruments. These disclosures shall include:

   i. All charges and fees associated with the use of the instrument.
   ii. The expiry period and the terms and conditions pertaining to expiration of the instrument.

b. Existing customer grivences redressal framework is applicable to all PPI products including designating a nodal officer to handle the customer complaints / grievances, the escalation matrix and turn-around-times for complaint resolution. The complaint facility, is also available on website / mobile, shall be clear and easily accessible. Which includes, at the minimum, the following:
   i. Shall disseminate the information of their customer protection and grievance redressal policy in simple language (preferably in English, Hindi and the local language).

ii. Clearly indicate the customer care contact details, including details of nodal officials for grievance redressal (telephone numbers, email address, postal address, etc.) on website, mobile wallet apps, and cards.

iii. Display proper signage of the customer care contact details as at (b) above.

iv. Provide unique complaint numbers for the complaints lodged along with the facility to track the status of the complaint by the customer.

v. Bank initiate action to resolve any customer complaint / grievance expeditiously, preferably within 48 hours and resolve the same not later than 30 days from the date of receipt of such complaint / grievance.

vi. Bank shall display the detailed list of their authorized / designated agents (name, agent ID, address, contact details, etc.) on the website / mobile app.

c. Bank shall create sufficient awareness and educate customers in the secure use of the PPIs, including the need for keeping passwords confidential, procedure to be followed in case of loss or theft of card or authentication data or if any fraud / abuse is detected, etc.

d. Bank shall clearly outline the amount and process of determining customer liability in case of unauthorised / fraudulent transactions involving PPIs. Bank PPI issuers shall also be guidedby the Department of Banking Regulation, RBI's circular DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 on Customer Protection Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.

e. Bank shall provide an option for the PPI holders to generate / receive account statements for at least past 6 months. The account statement shall, at the minimum, provide details such as date of transaction, debit / credit amount, net balance and description of transaction. Additionally, the PPI issuers shall provide transaction history for at least 10 transactions.

f. Customers shall have recourse to the Reserve Bank- Integrated Ombudsman Scheme, 2021 (as amended from time to time) for grievance redressal.

g. Bank shall ensure transparency in pricing and the charge structure as under:

i. Disclosure of charges for various types of transactions on its website, mobile app, agent locations, etc.
ii. Ensure uniformity in charges.
iii. Specific agreements with agents (if any) prohibiting them from charging any fee to the customers directly for services rendered by them on behalf of the Bank
iv. Require each retail outlet / sub-agent to post a signage indicating their status as service providers for the Bank and the fees for all services available at the outlet.
v. The amount collected from the customer shall be acknowledged by issuing a receipt (printed or electronic) on behalf of the Bank.

h. Bank shall be responsible for addressing all customer service aspects related to all PPIs (including co-branded PPIs) issued by the bank as well as it's agents.

i. Bank shall also display Frequently Asked Questions (FAQs) on their website / mobile app related to the PPIs.

j. PPI issuer shall also be guided by the following DPSS circulars:
   i. Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised Payment Systems issued vide DPSS circular DPSS.CO.PD No.629/02.01.014/2019-20 dated September 20, 2019 (as amended from time to time);
   ii. Online Dispute Resolution (ODR) system for resolving customer disputes and grievances pertaining to digital payments, using a system-driven and rule-based mechanism with zero or minimal manual intervention, issued vide DPSS circular DPSS.CO.PD No.116/02.12.004/2020-21 dated August 6, 2020 (as amended from time to time).

16. Limiting liability of customers in unauthorised electronic payment transactions in PPIs issued by bank:

a. Bank shall continue to be guided by RBI circulars DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017 or DCBR.BPD.(PCB/RCB). Cir.No.06/12.05.001/2017-18 dated December 14, 2017, as applicable on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.
b. Face-to-face / Proximity payment transactions: Transactions that require physical PPIs to be present at the point of transactions e.g. transactions at ATMs, PoS devices, etc.
c. The above shall be clearly communicated to all PPI holders.

17. Standard Operating Procedure:

Bank shall issue comprehensive SOP for Issuance of PPI, renewal on expiry, Issuance of duplicate PPI instruments, PPI limits, PPI features, PPI charges, handling of PPIs, handling of customer complaints/grievances etc. and FAQs from time to time.

18. Reference:

a. RBI Circular no DBS.CO.ITC.BC.NO.6/31.02.008/2010-11 dated 29th April 2011 regarding dated 29.04.2011 regarding Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of Recommendations.
b. RBI Circular no DBOD.No.FSD.BC.67/24.01.019/2012-13 dated 12.12.2012 regarding Issuance of rupee denominated co-branded pre-paid cards.
c. RBI Circular no DBS.CO/CSITE/BC.11/33.01.001/2015-16 dated 02.06.2016 regarding Cyber Security Framework in Banks.
d. RBI Circular no DBR.No.Leg.BC.78/09.07.005/2017-18 dated 06.07.2017 regarding Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions
e. RBI Circular no RBI/2015-16/164 DPSS.CO.PD.No.449/02.14.003/2015-16 August 27, 2015 dated 25.05.2019 regarding Cash Withdrawal at Point-of-Sale (POS) - Enhanced limit at Tier III to VI Centre’s

f. RBI Circular no RBI/DPSS/2017-18/58 Master Direction DPSS.CO.PD.No 1164/02.14.006/2017-18 dated 29.12.2017 regarding Policy Guidelines on issuance and Operations of pre-paid Payment Instruments in India.

g. RBI Master Directions on Prepaid Payment Instruments (PPIs), RBI/DPSS/2021-22/82 CO.DPSS.POLC.No.S-479/02.14.006/2021-22 dated 27th August 2021, updated on 12th November 2021.

h. RBI direction on Issuance of PPIs to Foreign Nationals / Non-Resident Indians (NRIs) visiting India, RBI/2022-23/176 CO.DPSS.POLC.No.S–1907/02.14.006/2022-23 dated 10th February 2023

i. Master Directions on Prepaid Payment Instruments (PPIs) (Updated as on February 23, 2024)

Chapter III

Merchant Acquisition

1. Preamble:

One of the important functions of the Bank is to provide Merchant Acquisition Services through its large network of branches across India. Any existing customer may avail the benefit of Bank of Maharashtra's Merchant Acquisition Services. In order to encourage banks to expand card acceptance / AEPS infrastructure to a wider segment of merchants across all geographical locations, RBI has advised vide letter no. RBI/2015-2016/410/DPSS.CO.PD. No./2894/02.14.003/2015-16 dated 26.05.2016 for formulation of Bank's own Board approved policy on merchant acquisition business.

2. Purpose:

This policy document on Merchant Acquisition Business outlines the guiding principles in respect of on-boarding of merchants on acquisition business, types of permitted transactions, discounting, settlement and dispute resolution. This policy shall apply to all the merchants' onboarding on various digital platforms initiated by the Bank. The policy shall be guided by Payment & Settlement systems act 2007. The document recognizes the rights of stakeholders and aims at dissemination of information with regards to various aspects of merchant acquisition business.

3. Stakeholders in Merchant Acquisition Business:

The main stakeholders in the Merchant Acquisition Business are as under:

a. Issuer: Card issuing institution/ issue bank
b. Cardholder: Customer/ non customer using card for making payment to merchant
c. Merchants: Entity which accepts payment through cards or any other digital channels
d. Acquirer: The bank that provides necessary infrastructure to the merchant to accept payment, maintain relationship and facilitate acceptance of payments through cards/ digital channels.
e. Intermediary Agency: Agencies who facilitate interbank settlements.
f. Card Issuing Bank: The financial institution/Bank which issues the card (Debit/ Credit Card/ Prepaid Cards to cardholder.
g. Card Associations: Institutions that provide Card Payment Network and facilitate clearing and settlement.
h. Regulator: RBI as a regulator of electronic payments in India.

4. Merchant Underwriting:

a. Acceptable criteria for Merchant/Aggregator/Master merchant underwriting are as under:
   i. Bank to verify the merchant (or its mobile application) on origin country and ownership for "foreign official/stakeholders" to conflict with regulatory/Government guidelines.

   ii. Clarity on permitted merchant types, segments and allocation of Merchant Category Codes (MCC) basis nature of business.

   iii. Validation of Merchant key information.

iv. Website/mobile merchant information screening to ascertain the nature of business.

v. Quantifying a new Merchant's financial risk exposure (e.g. Sales, volume, bureau checks, dispute history, delivery method, contingent liability) wherever applicable.

vi. KYC validation, sanction screening, other verifications, wherever applicable, as may be required.

vii. Assessing compliance with applicable data security standards and requirements.

viii. Conditions that require a Merchant to be re-underwritten (location, change in ownership, change in average sales volume/transaction amount, change in products/services offered etc.)

b. Merchant criteria- Bank shall classify merchants into Critical, High, Medium & Low risk segments so that appropriate oversight, monitoring and due diligence is suitably carried out on a periodic basis.

c. Prohibited Merchants-

i. Exclusion of merchant categories that have been banned under the Central or State laws and regulations as may be applicable.

ii. Exclusion of Merchant operating such business that is not specifically permitted by the regulator, statutory or any other competent authority.

iii. Exclusion of Merchant posing a high brand (or reputational) risk.

iv. Exclusion of Merchant operating in financial products/services that are not regulated.

5. Merchant On-boarding:

Merchant Acquisition Business is primarily referred to as the mechanism of providing necessary infrastructure and facilitating payments for goods and services purchased through medium of point of sale (POS), Bharat QR Code, VPA of UPI and IMPS. Bank has already initiated the process to set up, manage and operate Merchant Acquisition Business by introducing POS/ EDC terminals, BHIM-Aadhaar Pay Solution, Bharat QR and Maha-e-Pay Solution.

Merchant Services shall mean handling of electronic payment transactions for merchants by the Bank. Merchant processing activities involve obtaining sales information from the merchant, receiving authorization for the transaction, collecting funds from the issuing Bank and sending payment to the merchant. The processing of sales transactions for merchants by the Bank does not directly affect the Bank's balance sheet except through settlement accounts and reserve balances. Merchant Processing is a business of high volumes and low profit margin.

Bank installs Electronic Data Capture (EDC) machine or Point of Sale (POS) terminal(s)/PIN Pads, QR Codes, Bharat QR Code, VPA of UPI, IMPS, Aadhaar payment system at merchant's outlet(s). It facilitates acceptance of payment from customers by providing biometrics or by swiping debit/ credit/ pre-paid card on the POS terminals/ PIN Pads or by scanning QR Code as sale proceeds of goods and services. Merchant Acquisition Services enable merchants to accept Biometrics or all Visa/ MasterCard/ RuPay cards, UPI, IMPS etc. for payment. In case of mobile instrument of merchant is infected with virus/ malware, the user credentials such as PIN, OTP or Internet Banking user ID may get compromised. To mitigate the risk, branches should direct the merchants to get the mobile instruments updated with latest anti-virus and

proper system should be put in place for regular notifications through various modes of communications such as WhatsApp Messages need to be put in place.

Bank should have appropriate agreement in place with each merchant/aggregator/service provided before any service is provided or activities are outsourced. Agreements should be reviewed from time to time and updated appropriately with changes, if any.

In case of change in linked account number, new QR code need to be generated and issued to merchant/customer.

Product and processes for merchant onboarding shall be reviewed annually by Bank.

Following are the pre-requisites for Merchant On-Boarding:

i) Types of Merchants:

As per RBI circular no. DPSS. CO. PD. No. 1633/02.14.003/2017-18 dated December 6th, 2017, RBI has restructured MDR based on Merchant Turnover rather than the present slab-rate based on transaction value. The merchant classification should be done as per RBI guidelines.

The definition of small merchant & other merchant shall undergo change immediately upon change by regulator in this regard. In addition to yearly turnover segmentation of merchants can also be done on based on the below criteria:

a) Line of business
b) Nature of entity
c) Age of business
d) Estimation of amount per transaction
e) Estimation of transaction volume

The list of prohibited products and services is attached as Annexure 2, which shall not be sold/offered by merchants.

ii) Eligibility Criteria

Branches have to ensure that the following eligibility criteria has been complied with before onboarding a merchant:

a. Account Holder: The merchant desirous of availing facility of POS/ EDC terminals, BHIM-Aadhaar Pay Solution, Bharat QR, IMPS, UPI and Maha-e-Pay Solution must be Saving/ Current / Cash Credit Account Holder of the Bank. Saving Bank account should be accepted in case of very small merchant viz. vegetable vendors, pan shops etc.

b. KYC Compliance: The merchant account must be KYC complied. The guidelines issued under extant policy on KYC / AML/ CFT/PML act and Grievances Redressal shall be followed for ensuring KYC compliance.

c. Business License/ Registration Number: It is necessary to obtain merchant's business license number or any other license or registration numbers that may be required to own and / or operate business activities. (For e.g. Shop Act License, VAT Certificate, Registration Certificate etc.) In case of small merchants, who do not have registration number/ license, the copy of Aadhaar/ PAN should be obtained.

iii) Merchant Risk Categorization

Bank shall classify merchants into Critical, High, Medium & Low risk segments so that appropriate oversight, monitoring and due diligence is suitably carried out on a periodic basis. Merchant's risk categorization shall be carried out on the basis of account's risk profile (on the basis of Know Your Customer).

Bank/Branch shall effectively control and reduce risk by understanding of the normal and reasonable activity and transaction pattern of the Merchant. However, the extent of monitoring shall depend on the risk sensitivity of the account. Bank/Branch shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

For purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Merchants belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, it is require that only the basic requirements of verifying the identity and location of the customer are to be met. Merchants that are likely to pose a higher than average risk to the bank shall be categorized as medium or high risk depending on merchant's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Branch shall apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence include

a) non-resident merchants;
b) high net worth individuals;
c) trusts, charities, NGOs and organizations receiving donations;
d) companies having close family shareholding or beneficial ownership;
e) firms with 'sleeping partners';
f) politically exposed persons (PEPs);
g) non-face to face customers and
h) those with dubious reputation as per public information available etc.

However, only NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer).

Branches shall recommend threshold limits for a particular merchant. The threshold limit shall be defined for each merchant at Head Office based on the Turnover of the account in previous 2 years. The threshold limit shall be reviewed by Head Office at a frequency of 6 months based on the monthly transactions volume. The branches shall be informed about the transaction limits fixed by Head Office for each merchant. If merchant breaches the transaction monthly limit by 20%, then transaction scrutiny shall be carried out by Head Office team. The findings shall be intimated to the branch and customer. Subsequently, the branch shall do due diligence and recommend Head Office for continuing the existing limit or enhancement in limit or discontinuation of service.

Head Office team handling Merchant acquisition shall prepare monthly report based on MCC, transactions volume, type, card type and appraise the same to the higher

authorities i.e. Chief Information Officer (CIO). Comments of higher authority shall be communicated to the branches.

The Reconciliation Team at DCRD (Digital Channel Reconciliation Department) comprising of one officer supervised by Chief Manager/Asst. General Manager shall scrutinize the transactions. In case of adverse findings based on analysis of daily transactions reconciliation team will immediately report the same to Chief Digital Officer (CDO)/ Chief Information Officer (CIO).

Process for identification of Large/Complex transactions:

a) Monitoring of daily transactions – Team of officers of DBD Department, Head Office shall extract daily reports of transactions for analysis.

b) Monitoring of large/complex transactions shall be done at minimum on the basis of following reports:

i. Declined Transaction Report -Transactions declined due to Security Violation, Pickup & Stolen Card, Expired and Restricted Card, Do not Honor etc.
ii. Manual key offline report (where transaction gets processed with the help of card number only) -Transaction done through Key Entry Mode – Card Absent environment.
iii. Tip transaction report –In this report, Team analyses cases where Tip Amount exceeds bill amount.
iv. Split Transaction Report –Same card swiped at same terminal for more than 3 times in a day
v. Settlement report (all transactions are covered in this report) –Suspicious transactions identified in the above reports are highlighted in the Settlement report
vi. Other Suspect Transactions Report - All international transactions, All transactions > Rs. 30000, All transactions between 00:00 Hrs to 8:00 Hrs.
vii. Transactions of newly On-Boarded merchants
viii. Transactions of newly On-Boarded merchants shall be monitored for 7 days. Based on which, the threshold & pattern of transactions shall be identified & set.

On the basis of aforesaid parameters, transaction monitoring team shall hold suspicious transactions in system before processing payment (credit) to the merchant and carry out investigations for suspicious or questionable transactions.

c) Post transaction hold activity – The merchant and concern branch shall be informed to submit invoice copy, card holder ID proof etc. to check the genuineness of transactions. On submission of a valid document, the payment shall be released.

iv) Risk Assessment

While merchant processing, it is required to understand and control primary risks i.e. chargeback, fraud and reputational risks. Failure to control these risks may result in loss for the Bank.

a. Chargeback Risk: The merchant may settle and get paid by the Acquirer for Sale transactions, which are subsequently prone to disputes or Chargebacks. If the

Merchant ceases to trade and/ or becomes insolvent or non-existent, recovery of such amounts charged-back by customers becomes challenging and the Acquirer is left with financial losses.

b. Fraud Risk: The merchant may create or accept fraudulent transactions, which are liable to be charged-back by the Issuing Banks. This can leave the acquirer severely exposed to financial losses.

c. Reputational Risk: This risk happens due to merchant involved in socially unacceptable or illegal products/services and/or dubious business practices. This may cause the Acquirer irreparable damage by virtue of mere association with such a Merchant.

All the above risks should be taken into consideration while establishing relation with a merchant to avoid financial or reputational loss to the Bank. To avoid the risk of financial and reputational loss to Bank, indemnity clause shall be incorporated in every agreement. Also clause on security of data by vendor for handling data while capture, transmission, storage and computation should be incorporated in every SLA. In case of any loss whether financial or reputational, aggregator shall be held responsible for the same.

Digital Banking Department should do yearly review of Inactive / Dormant merchants.

v) Investigation

If the investigation reveals Merchant involvement in illegal and/or fraudulent activity or in any other brand damaging activity, the Bank must:

a. Take appropriate legal action to minimize losses and explore other legal remedies.
b. Hold any and all available settlement funds, if any.

6. Minimum Standards:

All industry stakeholders who process and /or store cardholder information shall ensure that their terminals, applications and processing systems comply with the minimum requirements of the following standard and best practices. All terminals, applications and processing systems should comply with the standards specified by the various card schemes. Bank should onboard only those vendors who have provided valid certificates showing compliance with these standards and must review status of all its terminals on monthly basis to ensure they are still compliant to the standards.

i) Payment Card Industry Data Security Standard (PCIDSS)

ii) Payment Application Best Practices (PABP)

iii) EMV

iv) Triple DES

v) Any other standards declared from time to time

vi) Adherence to RBI’s master direction on Digital Payment Security Controls vide DoS.C.O.CSITE.SEC.no.1852/31.01.015/2020-21 dt.18.02.2021.

The monthly report shall be prepared and submitted to the General Manager/Dy. General Manager DBD by the concerned team of Digital Banking department.

Digital Banking department should maintain and circulate the minimum standards to Branches and Merchants.

7. Types of Point of Sale (POS):

Bank provides following type of terminals / channels to suit merchant's needs:

7.1 POS / EDC Terminals

A point of sale terminal (POS terminal) is an electronic device used to process card payments at retail locations. Following are types of POS terminals:

a) PSTN: Public Switched Telephone Network based POS machines
b) GPRS: General Packet Radio Service based POS machines
c) Mobile POS: Wireless mobile type M-PoS instrument

7.2 QR Code

QR code or Quick Response code is a two-dimensional machine-readable code that is made up of black and white squares. It is used to store Merchant ID (RuPay, VISA), UPI-VPA, Merchant Name, and other information such as URL, Aadhaar number, MCC, etc.

a) Maha-e-Pay: A digital way of payment using static QR codes.

b) Bharat QR: Bharat QR Code is the world's first inter-operable payment acceptance solution. Bharat QR code aims at standardizing the QR code payment method through the country. Payment networks such as MasterCard, American Express and Visa have collaborated with National Payment Corporation of India (NPCI) to launch and promote the Bharat QR payment method. However, different merchant outlets across the country uses different QR codes.

c) BHIM UPI QR: BHIM (Bharat Interface for Money) is a mobile app developed by National Payments Corporation of India (NPCI), based on the Unified Payment Interface (UPI). User can make instant bank-to-bank payments and pay/ collect money using Mobile number, Bank account number and IFSC Code, Aadhaar number or Virtual Payment Address (VPA).

BHIM has the facility to Scan & Pay through QR code. User can check transaction history and can also raise complaint for the declined transactions by clicking Report issue in transactions. BHIM is available in 13 regional languages i.e. English, Hindi, Marathi, Tamil, Telugu, Bengali, Malayalam, Oriya, Gujarati, Kannada, Punjabi, Urdu and Assamese for better user experience.

7.3 BHIM Aadhaar Pay

Aadhaar-pay is based on AEPS system (Aadhaar Enabled Payment System), which has already been implemented in most of the Banks. AEPS utilizes the biometrics of a person in order to authenticate and authorize the transactions. Aadhaar pay enables the merchant to use his Smartphone along with a biometric scanner attached as a POS machine. Banks are required to provide a mobile app for merchants as per the specifications laid down by NPCI.

7.4 **BHIM**

BHIM is an initiative to enable fast, secure, reliable cashless payments through your mobile phone. BHIM is interoperable with other Unified Payment Interface (UPI) applications and bank accounts for quick money transfers. BHIM app is developed by National Payments Corporation of India (NPCI).

7.5 **BHIM UPI**

The Unified Payments Interface (UPI) offers architecture and a set of standard Application Programming Interface (API) specifications to facilitate online payment. It aims to simplify and provide a single interface across all NPCI systems besides creating interoperability and superior customer experience.

8. Types of Transactions:

Transactions can be performed using debit cards, credit cards, scanning QR codes, AEPS (Aadhaar Enabled Payment System), contactless cards. Details of the same are provided below:

a. **Card Based Transactions**

This type of transactions involves card holders and their Banks (Issuer) on one hand, Merchants and their Banks (Acquirers) on the other hand and a payment network (Visa/ MasterCard) in the middle that co-ordinates the flow of information and money underlying the transaction. The transactions are validated through “PIN” of the cardholder.

b. **Card less Transactions**

This type of transactions can be carried out without using debit / credit cards. QR code based transactions, AEPS, contactless cards transactions fall under this category. Details of the same are given below:

i. QR Code Based Transactions: Under this type of transactions, customer can make payment by scanning the QR code. Customer has to enter the amount and select the payment mode i.e. Debit/ credit card, net banking or wallet.
ii. AEPS (Aadhaar Enabled Payment System): AEPS utilizes the biometrics of a person in order to authenticate and authorize the transactions.
iii. Contactless Cards: These cards work on Near Field Communication (NFC) technology using radio transmission to ascertain contact when the card is brought near a terminal. As no signature or PIN verification is required, contactless purchases are typically limited to a set maximum limit as per Govt./RBI directions.

9. International Merchant Acquisition:

International merchant acquisition refers to payment solutions that give e-commerce businesses the ability to accept credit card payments from consumers around the world. Presently International Merchant Acquisition is not undertaken by the Bank. In the near future, if regulatory authorities directs for international merchant acquisition, the policy should be reviewed in the said context.

10. Security:

The Point of Sale (POS) related transactions originating from the merchant's site shall be routed to NPCI/ VISA/ Master Card payment network through the switch of the service provider. The service provider has to be a PCI DSS certified company & should have necessary interface with Bank Card Associations. The data between the service provider & Bank shall flow through a secured channel i.e. secured file transfer protocol (SFTP). The network infrastructure for routing of transaction shall be provided by the service provider & the Bank shall put in place its own infrastructure to manage the business e.g. underwriting of merchants, settlement of fund, reporting & control & risk management.

Customers should also ensure security of device and updating anti-virus to avoid risk of comprise of credentials such as card details and OTP.

Bank to deploy web crawler scan services to determine whether the products or services offered are inconsistent with the Merchant's transaction activity, wherever its applicable.

a. Changes in the type of products offered that effectively alter the Merchant's MCC.

b. Transaction laundering by misusing the credential and resulting in illegal sale of products / services.

c. To identify potential violations involving sale of banned goods / controlled substances / illegal services and unethical business by the merchant.

11. Aggregators / Partners:

Aggregators are payment service providers who provide Bank's Payment Solution Services to multiple merchants. For the purposes of this policy, the Aggregators shall be as below:

a. Aggregator offering payment solutions and act as payment facilitator to enable merchants to accept card payments using Electronic Data Capture- POS and /or Online Payment Gateway

b. In order to enable the merchants for such payment gateway facilities Bank may facilitate integrations / on-boarding of these merchants on the aggregator platform.

c. Aggregator supplying and maintaining EDCs, POS etc. and providing transaction processing for Merchant Acquisition Business summarily called Payment Solution for establishments/merchants in respect of payments sought to be made by Customers by way of debit/ credit cards.

d. Aggregator providing Merchant Payment Platform for Aadhaar Based merchant payment from a single device. It consists of Mobile Application for Merchant payment transactions that can be offered to Merchant Application Payment Gateway.

e. These aggregators agree to pay to the Merchant Payments (Authorized or Approved) within the time frame decided by VISA/ NPCI & NPCI except under circumstances beyond the reasonable control of it.

12. Discount Policy / MDR:

To facilitate digital transactions, the Merchants have to set payment infrastructure like POS (Point of Sale) machines and have to start a unique account which is called merchant account with a bank to avail payments from the customers. As the bank provides payment services, the merchants have to pay to the bank for using payment infrastructure set up by the Bank. This payment is referred to MDR (Merchant Discount Rate).

With a view to provide further fillip to acceptance of debit card payments for purchases of goods and services across a wider network of merchants, Reserve Bank of India has decided to rationalize the framework for Merchant Discount Rate (MDR). Rationalization of MDR to be done based on following:

a) Categorization of merchants on the basis of turnover
b) Adoption of differentiated MDR for QR code based transactions
c) Specifying ceiling on the maximum permissible MDR for both 'Card based and Card less transactions"

Merchants on-boarded by Bank should not pass on MDR charges to customers while accepting payments through debit cards. Rationalization of MDR as modified by RBI from time to time shall be applicable on all merchant acquisition. The MDR levied on the merchant shall not exceed the cap rates prescribed by RBI, irrespective of the entity which is deploying the card acceptance infrastructure at the merchant location.

13. Delisting and de-activation of merchants:

Guidelines on the delisting of and de-activation of merchants to be referred from SOP for the same. Digital Banking Department shall undertake review of their operations/issue and inactive merchants on yearly basis and review report to be put to competent authority for necessary decision on issues and deactivation of QR codes.

14. Merchant training:

a. Bank to create ongoing training module with Merchants on the acceptance methods and guidelines.
b. Training to be conducted physically / virtually with adequate information in line with the policy of the Acquiring Member Bank
c. FAQ's along with Do's and Don'ts to be published by the Bank.

15. Third party agent oversight and governance:

a. Bank should do necessary underwriting as may be required for on-boarding of any third party service provider.
b. Bank should conduct a periodic review/audit of the third parties engaged by the Merchant/s.
c. Bank should establish controls in line with outsourcing policy.

16. Record Keeping:

Record for all the merchants transactions to be retained as per Record retention policy of the bank.

17. Standard Operating Procedure:

Bank shall issue comprehensive SOP for Pre-Installation process, Merchant QR limits, Merchant QR features, Merchant QR charges, handling of merchant QR, handling of customer complaints/grievances, Settlement & reconciliation, Merchant training etc. and FAQs from time to time.

18. References

a. RBI Letter No RBI/2015-2016/410/DPSS.CO.PD.No./2894/02.14.003/2015-16 dated 26.05.2016
b. RBI circular no. DPSS. CO. PD. No. 1633/02.14.003/2017-18 dated December 6th, Dec 2017
c. Bank circular no AX1/Inspection & Audit /KYC-AML-CFT Policy/2022-23 on "KYC/ AML/ CFT Policy" dated 28/06/2022
d. Bank circular no AX1/PLN/KYC/Cir.No.41/2017-18 on "PML act amendment 2017: Revised KYC Guidelines" dated 26/09/2017
e. Bank circular no AX1/Customer Service/2022-23 on "Customer Service Policy" dated 28/06/2022 comprises of Compensation Policy and Grievances Redressal Policy.
f. NPCI Guidelines for members on Merchant acquisition standards NPCI/UPI/Rupay/OC-118/2021-22 dated 08/09/2021

19. Enclosures

Annexure 1 – Important Terms & definitions
Annexure 2 – List of prohibited products and services
Annexure 3 – List of avoidable Merchant Categories

20. Annexure 1: Important Terms / Definitions:

The recitals, Schedules and Annexures to this policy shall form part of this policy as if incorporated in verbatim in the body of this policy.

a) Merchant Discount Rate: The commission charged by the acquirer to the Merchant. It is also termed as Merchant Service Fees (MSF)

b) Interchange: The incentive paid by the Acquirer bank to the card issuer bank for promoting payments through cards.

c) Scheme Fees: The service fees paid to intermediary agencies i.e. MasterCard or VISA for facilitating interbank payments.

d) On-Us Transactions: Where issuer and acquirer is same (e.g. BOM Debit Card and BOM POS Terminal)

e) Off-Us Transaction: Where issuer and acquirer are different (e.g. other bank's debit/credit card on our POS Terminals)

f) Acquiring Bank: A bank that contracts with merchant for the settlement of card / AEPS transaction is an acquiring Bank.

g) Issuer Bank: A bank that holds customers account in any form i.e., Saving/ Current /debit card/ credit card/ etc. is issuer bank.

h) EDC/POS Terminals shall mean PSTN, GPRS, PC POS, MPoS, QR Code, BHIM Aadhaar Pay, BHIM UPI, BHIM, etc. to be installed at Merchant Locations for acceptance of all types of cards, issued in association with VISA, MasterCard & NPCI(also AMEX, if desired by the bank), AEPS etc.

i) BHIM UPI: The Unified Payments Interface (UPI) offers architecture and a set of standard Application Programming Interface (API) specifications to facilitate online payment. It aims to simplify and provide a single interface across all NPCI systems besides crating interoperability and superior customer experience.

j) BHIM Aadhaar Pay: It is easiest and cheapest method of payment. It uses the customer's fingerprints for authentication. On the basis of authentication, the money will be paid to merchant from customers Aadhaar linked account.

k) Bharat QR Code: The Bharat QR code is a result of the initiative of the Government of India. Bharat QR code will enable the merchants to accept digital payments without the Point of Sale (PoS) swiping machine. It will allow customer of any bank to use their smartphone application to make payment using their UPI or debit / credit cards.

l) Customer Order: It means an order for purchase /acquisition of the Product(s) offered by the merchants where the payment for the Product (s) is done through the Bank POS.

m) Payment Solution: It means the processing of transactions and payments sought to be made by Customers by way of debit/ credit/ prepaid cards / QR Code/ AEPS through the Bank POS that will be provide by the Bank to enable the Authentication

of Customers and Authorization of payments on Valid Cards/AEPS in accordance with Payment Mechanism.

n) Valid Card: It means an unexpired debit or credit card issued by any institution designated to issue a Rupay, Visa, MasterCard, Visa Electron or a Maestro or other card as may be specified by AGS from time to time provided that the card is not listed in a current warning or restricted card bulletins or notices and bears the signature of the person in whose name the card is personalized.

o) Merchants: It mean merchants on-boarded from time to time by Bank

p) BIN: It means Bank Identification Number, which are obtained from Card Schemes by the Bank used exclusively to process transactions.

21. Annexure 2 – List of prohibited products and services

Indicative list of prohibited products and services:

1. Firearms or Explosives or pyrotechnic devices or supplies

2. Adult services which includes pornography and escort or prostitution services

3. Website access and / or website memberships of pornography or illegal sites

4. Live animals, endangered species, which includes plants, animals

5. Banned / illegal drugs or other controlled substances or drug accessories and Miracle cures

6. Hazardous materials, combustibles, corrosives

7. Bulk email software or Bulk marketing tools or Multilevel marketing collection fees or Work-at-home approach

8. Gaming/gambling which includes lottery tickets, sports bets, memberships/ enrolment in online gambling sites, etc.

9. Matrix sites or sites using a matrix scheme approach

10. Mailing lists

11. Internet pharmacies

12. Fake products or autographs

13. Body parts which includes organs or other body parts

14. Cable descramblers and black boxes which includes devices intended to obtain cable and satellite signals

15. Copyright unlocking devices, copyrighted media, copyrighted software

16. Government IDs or documents which includes fake IDs, passports, diplomas, and noble titles;

17. Hacking and cracking materials

18. Offensive goods, which includes literature, products or other materials that: a) Defame or slander any person or groups of people based on race, ethnicity, national origin, religion, sex, or other factors b) Encourage or incite violent acts c) Promote intolerance or hatred;

19. Offensive goods, crime that includes crime scene photos or items, such as personal belongings, associated with criminals;

20. Hazardous materials which includes fireworks and related goods; toxic, flammable, and radioactive materials and substances;

21. Tobacco and cigarettes

22. Traffic devices, which includes radar detectors/hammers
23. Weapons including firearms, ammunition, knives, brass knuckles, gun parts,
24. discounted currencies or currency, exchanges;
25. Any product or service, which is not in compliance with all applicable laws;

22. Annexure 3 - Indicative List of avoidable Merchant Categories

1. Telephone Based Selling (also called Audio-Text): This involves high-pressure selling tactics/ exaggerations and often false promises.

2. Timeshares: Very long fulfillment period.

3. Pyramid Selling/Multi-Level-Marketing Companies: High Pressure selling techniques can result in customer dissatisfaction, resulting in disputes / Chargebacks.

4. Dating/Escort Agencies: Customers can Chargeback transactions due to unhappiness with quality of introductions.

5. Betting/Gambling/Lotteries/Games of Chance/Sweepstakes: Restrictions by RBI.

6. Health Elixir Sales/ Beauty & lifestyle products/ Beauty therapies and parlors offering the same: Exaggerated claims of beauty, reversal of age, attainment of youthfulness etc. These services/ products are very personal in nature, and are not quantifiable, thus leading to cardholder dissonance and disputes.

7. Massage Parlors: Often conduct unethical/ unlawful businesses, which can damage the Acquirer's reputation by implication.

8. Merchants dealing in Illegal/ unlawful Merchandise: Examples include pet shops which deal in trading of endangered/ protected birds/animals. Merchants dealing in Pornographic or the so-called Adult/Mature material also fall under this category.

9. Intangibles: Example of this includes software downloaded via the Internet. In case of Chargebacks, it is often very difficult to prove that the Software could be downloaded and installed successfully/correctly by the user

Note: Branches are required to do due-diligence while selection of merchant and it should be responsibility of the branches not to select merchant from avoidable Merchant Categories.

Chapter IV

ATM and Recycler

1. Preamble:

One of the functions of the Bank is to install and operate ATMs/Recyclers at onsite and offsite locations identified by the Bank. RBI vide its circular no. BAPD.BC.72/22.01.001/2015-16 dated 14.1.2016 have provided operational freedom to banks, with regard to offering of various products and services through the ATM channels provided the technology permits the same, and adequate checks are in place to prevent any misuse of the ATM channel.

Bank would adopt and follow the RBI and Govt. guidelines like Control measures for ATMs, Cassette Swap in ATMs, Security measures for ATMs, Monitoring availability of cash in ATMs etc., issued from time to time for operating ATMs and Recyclers.

2. Purpose:

This policy document on ATM and Recycler outlines the guiding principles in respect of operation, monitoring, maintenance and upkeep of ATMs and Recyclers of Bank of Maharashtra. issuance of Small PPIs and Full-KYC PPIs payment instruments, types of permitted transactions, discounting, settlement and dispute resolution in Bank of Maharashtra.

3. Definitions:

a. **Automated Teller Machine (ATM):** An ATM is a computerized machine that provides customers of banks the facility of accessing their accounts for dispensing cash and to carry out other financial & non-financial transactions without the need to visit the bank branch.

b. **Cash Recycler (CR)**: The Cash Recycler machine (CR) is a self-service terminal that lets you and me to make deposit and withdrawal transactions of cash. All successful transactions are immediately credited or debited in real time and customers will be issued an acknowledgment slip confirming the transaction.

c. **Personal Identification Number (PIN):** PIN is the numeric password which is separately mailed / handed over to the customer by the bank while issuing the card. Most banks require the customers to change the PIN after the first use. Customers should not disclose PIN to anybody, including to bank officials. Customers should change the PIN at regular intervals.

d. **On-Us and Off-Us transaction:** A transaction carried out at an ATM of the card issuing bank is called an On-Us transaction. A transaction carried out at any other ATM is called an Off-Us transaction. For instance, if a card issued by BoM is used at an ATM of BoM then it is an On-Us transaction; if the card is used at an ATM of any other bank, the transaction is Off-Us.

e. **Remote On-Us transaction**: A transaction carried out at an ATM other than card issuing bank is called a Remote On-Us transaction. For instance, if a card issued by BoM is used at an ATM of other Bank then it is a Remote On-Us transaction.

f. **Regulator:** RBI regulates the electronic payments in India.

4. Classification of ATMs/CRMs:

a. The ATM Classification will be on the same lines as Branch Classification of Metro, Urban, Semi Urban and Rural.

b. ATMs/CRMs are deployed under Capex and Opex models. Under Capex Model, ATM/CRM is owned by the Bank and site is developed and maintained by the Bank. Whereas under Opex model (also known as End to End (E2E)/Ministry of Finance (MoF) ATM) the ATM is owned by the outsourced vendor and site is developed and maintained either by the Bank or by vendor.

5. Services Provided through ATM/CRM:

Following services are provided through Bank ATM/CRM

a. Cash Deposit (through CRM)/ Cash Withdrawal
b. Green Pin Generation and Personal Identification Number (PIN) changes
c. Card-less Cash Withdrawal
d. Requisition for cheque book
e. Mini Statement of accounts
f. Balance enquiry of accounts
g. Utility payments like Mobile recharge, Telephone bill etc.
h. Product Information of retail products and display of educative creative's
i. Aadhaar seeding in accounts
j. Intra Bank Fund transfer – Card to Card and Card to Account.
k. Interoperable Card less Cash Withdrawal (ICCW)

6. Digital Gallery

a. Digital gallery shall act as extension counter for digital services and it shall be linked to nearby Branch.

b. Digital gallery shall be equipped with:
   i. ATM
   ii. Cash Recycler
   iii. Passbook Kiosks or Multi-Function Kiosk

c. Digital gallery shall be available 24 X 7 for customer convenience.

7. Site Selection:

a. The parameters to be considered while finalizing location of offsite ATM is, expected number of hits, vantage location and visibility. While selecting off site locations, care should be taken to identify Issuer transaction location (i.e. our card holders using other Bank ATMs).

b. Selection of On-Site ATM locations will be done at the time of opening the Branch by the respective Zonal Offices or subsequently for existing branches on attaining potential.

c. Zonal office should ensure that all Branches of Bank should have an onsite ATM/CRM.

8. Site Specifications & Premises:

a. Space requirement is 80-100 SQFT with 10% deviation on optimum area (As per Premises Policy issued by Corporate Services department) on the ground floor and main road, easily accessible to large number of public and in near vicinity of reputed offices, institutes, Malls having satisfactory footfalls, Railway Stations/ Bus Depots, Air Ports, busy Market / commercial areas, etc. The sites should not be in secluded places or places restricted to public. Bank can deploy Window ATMs if sufficient space is not available for deployment of normal ATMs/CRMs

b. Completion of site preparation work Availability of Ramp at ATM as per DFS guidelines so that the persons with disabilities / wheel chair users can enter the ATM centers and conduct business without any difficulty.

c. Availability of UPS power, RAW Power and LAN connectivity (data cabling and I/O points). LAN/Power points/cables should be concealed or affixed inside the backroom to avoid fraudulent attempt. Zonal Office to ensure strict compliance of the same.

d. All ATM/CRM sites should be equipped with E-Surveillance system with 24X7 monitoring for safety and security of customers and ATM/CRM site.

e. The Off/On site ATMs should have pleasant ambience and if air-condition is not feasible then ceiling & exhaust fan should be provided. It should be well stocked with Bank's promotional brochures / pamphlets.

f. ATM should be placed in such a way that other customers should not be able to see the PIN entered by the ATM users.

9. Settlement and Reconciliation

a. In respect of fully outsourced ATMs, the service provider will be responsible for reconciliation of Physical cash with balance in Cash at ATM as per ATM-Switch and submission of reconciliation certificate to DCRD Team. DCRD team will verify the reconciliation certificate submitted by service providers. DCRD team will inform the shortages to payment section for recovery from service provider. However, link branch officials will also verify the physical cash with the balance in Cash at ATM-Switch at least once in a month.

b. In respect of all the ATMs where cash replenishment services are outsourced to a service provider, the service provider must tally the cash on load to load basis. In addition, the link branch is expected to physically verify the cash balance once in a month with ATM counters.

c. Inspection and Audit Department is responsible for monthly physical cash verification of ATMs/CRMs.

d. Settlement and reconciliation procedure shall be followed for all the transactions carried out at ATMs/CRMs by Digital Channel Reconciliation Department.

e. The settlement shall be carried out as per RBI directives on Harmonization of Turn Around Time (TAT) and customer compensation for failed transactions. The required transaction data logs from various entities including ATM Switch, Vendors, CBS, Branches etc. should be obtained and processed.

10. ATM Site Maintenance

a Capex Model (Bank owned) ATMs will be maintained by the Managed Services Vendors (MS vendors) and Opex model (owned by vendor) ATMs will be maintained by the respective vendors

b The ATM site has to be always maintained neat, tidy and properly illuminated. Branch/Zonal Offices should ensure that the same is maintained.

c Monitoring of the down ATMs, upkeep of sites is the primary responsibility of the link branch and Zonal Office.

d All Capex ATMs/CRMs shall be adequately insured by Corporate Services Department, Head Office with "Electronic Equipment Policy" which included insurance cover for fire and allied perils, RSMD (riot, strike, malicious damage), earthquake, STFI (storm, tempest, flood, inundation), short circuit and electrical fire including mechanical and electrical, smoke, soot, dust, corrosive gases etc., water and humidity, terrorism and burglary.

e On relocation /closure of the ATMs, link branch/vendor should ensure to take existing hard disk and hold the same for future reference in case of dispute. The ATM shall also be transferred to the new site after dismantling and removing all the infrastructure from existing site.

f The procurement & payment of ATMs/ CRMs shall be made centrally as per procurement policy and the asset will be controlled at respective Branches'.

11. Economics

a. In order to make the ATM economically viable and in keeping with existing Industry standards, endeavor should be to generate 100 plus hits per day within 6 months of installation. After installation of the ATM, the Zonal Office should closely monitor the minimum daily hits. In case ATM is not getting 100 + hits daily after 6 months of installation, Zonal Office should ensure to take all the required steps for improving the hits, which may include relocating the ATM (In case of offsite) to a viable location within next 3 months.

b. Bank earns revenue if Card Holders of other Banks use our ATM. The location therefore should be such that it attracts even other bank cardholders.

c. In the normal course the installation should have positive benefits, however in exceptional cases like prestigious location / valuable connection, the same can be considered on case to case basis. The same should be fully justified by the Zonal office.

12. ATM/CRM Operation

a. Digital Banking Department at HO will monitor and maintain the uptime of ATMs/CRMs as per the SLA clause in coordination with respective MSPs and Branches.

b. Digital Banking Department shall ensure timely reporting of addition/deletion of ATMs/CRMs in ATM-Switch and Digital Channel Reconciliation Department.

c. Digital Banking Department shall make available hardware / software /service providers for implementation of lockable cassettes for cassette swap method and OTC for cash replenishment.

d. Digital Banking Department shall place requirement of ATM/CRM to Information Technology Department well in advance to complete the procurement process.

e. Linked Branches shall ensure intimation of insurance claim for ATM/CRM within 90 days of incident and submission of all required documents for settlement of insurance claim.

13. Cash Replenishment

a. The cash will be replenished by Branch officials for ATMs under Capex Model at onsite locations and by CRA designated by respective vendors under Opex model and offsite ATMs/CRMs under Capex model.

b. Nodal Branches / Currency chest will issue cash to Cash Replenishing Agencies (CRAs) by debiting respective Cash at ATM accounts up to 12 Noon so that cash loading activity is necessarily completed on the same day. Custodian of the ATM/CRM has to do admin job mandatorily at the time of loading of cash. The amount of cash to be deposited in the ATM should be as per the limit fixed for each ATM from time to time.

c. The Cash held in ATM should be such that it should neither be excess resulting in idle cash balance nor less which will lead to cash out position resulting in non-dispensing of cash. Cash feeding should be based on the forecast given by the vendor on day to day basis for both On site and Off site ATMs wherever cash is replenished by the vendor.

d. It will be the responsibility of the Branch to which the ATM is attached to ensure that adequate cash is always available in the ATM to meet the needs of the customers.

e. ATMs at Onsite locations, Cash replenishment will be done by the respective branch custodians and FLM will be done by MS vendor & branch custodian.

f. Currency chest / Branch should ensure that only properly sorted and examined ATM fit notes are put into circulation through the ATM/CRM.

g. ATM CASH OUT: RBI has advised that the Banks shall strengthen their systems/mechanisms to monitor availability of cash in ATMs and ensure timely replenishment to avoid cash-outs. Any non-compliance in this regard shall attract monetary penalty, which is effective from October 01, 2021. It is advised by RBI that Banks shall submit system generated report of ATMs which were cash-out for more than 10 hours in the month to the Issue Department of RBI under whose jurisdiction these ATMs are located. Cash-out of any ATM for more than 10 hours in a month will attract a flat penalty of Rs 10,000/- per ATM. Branches /Zonal Offices shall ensure that ATMs are not going cash out and shall regularly check the cash report shared by ATM Switch team and ATM Team HO. Digital Banking Department shall provide the monthly system generated ATM Cash out report after making necessary changes in the report for correctness and duly approved by Auditor to Zonal offices. Zonal office shall submit report to respective ID of RBI on or before 5th day of succeeding month. Zonal office shall coordinate with their respective Issue Department of RBI for any waiver and appeal, if any, in time.

h. Digital banking Department shall ensure that Cash replenishment in all ATMs should be done through digital One Time Combination (OTC) lock using dynamic

password shared by the Central Server from the back end with the custodians of the ATM to secure the Cash replenishment activity.

i. As per Cassette swap method, ATM cash replenishment will be done by exchanging the cassette in ATM with a prefilled locked cassette with cash to mitigate the risk of tampering of cash.

14. Security, Fraud prevention and Risk Management Framework:

a. Bank shall put suitable controls to implement RBIs guidelines on Control measures on ATMs.

b. Bank shall implement terminal security solution in order to enhance the ATM security.

c. Bank shall ensure to implement necessary controls to comply with RBI advisory on Man in the Middle (MiTM) Attacks in ATMs.

d. A strong risk management system is necessary for Bank to meet challenges of fraud and ensure customer protection. Bank shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.

e. To meet the challenges of fraud and ensure customer protection. Bank shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.

f. Bank shall also put in place suitable mechanism to prevent, detect and restrict occurrence of fraudulent transactions through ATMs/CRMs.

g. Bank shall put in place suitable internal and external escalation mechanisms in case of suspicious operations, besides alerting the customer in case of such transactions.

h. Where direct interface is provided to their authorised / designated agents, Bank shall ensure that the compliance to regulatory requirements is strictly adhered to by these systems also.

i. Bank shall establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. Any such incident should be reported to CISO for onwards submission to RBI/Cert-IN. The same shall be reported immediately to DPSS, RBI, Central Office, Mumbai. It shall also be reported to CERT-IN as per the details notified by CERT-IN.

j. Bank's Security department shall ensure all ATMs/CRMs premises shall have E-surveillance system including their maintence.

15. Customer Protection and Grievance Redressal Framework:

a. Bank shall disclose all important terms and conditions in clear and simple language (preferably in English, Hindi and the local language) to the customers using ATM/CRM of Bank. These disclosures shall include:

   i. All charges and fees associated with the use of the ATMs/CRMs.
   ii. Details for handling customer Grieviance pertaining to failed transactions.

b. Existing customer grivences redressal framework is applicable to ATMs/CRMs including designating a nodal officer to handle the customer complaints / grievances, the escalation matrix and turn-around-times for complaint resolution. The complaint facility, is also available on website / mobile, shall be clear and easily accessible. Which includes, at the minimum, the following:

i. Shall disseminate the information of their customer protection and grievance redressal policy in simple language (preferably in English, Hindi and the local language).
ii. Display proper signage of the customer care contact details.
iii. Provide unique complaint numbers for the complaints lodged along with the facility to track the status of the complaint by the customer.
iv. Bank initiate action to resolve any customer complaint / grievance expeditiously, preferably within 48 hours and resolve the same not later than 30 days from the date of receipt of such complaint / grievance.

c. Bank shall create sufficient awareness and educate customers in the secure use of the ATM/CRM, including the need for keeping passwords confidential, procedure to be followed in case of loss or theft of card or authentication data or if any fraud / abuse is detected, etc.

d. Customers shall have recourse to the Reserve Bank- Integrated Ombudsman Scheme, 2021 (as amended from time to time) for grievance redressal.

e. Bank shall ensure transparency in pricing and the charge structure as under:

i. Ensure uniformity in charges.
ii. Disclosure of charges for various types of transactions on its website, mobile app, agent locations, etc.
iii. Specific agreements with agents (if any) prohibiting them from charging any fee to the customers directly for services rendered by them on behalf of the Bank
iv. Require each retail outlet / sub-agent to post a signage indicating their status as service providers for the Bank and the fees for all services available at the outlet.
v. The amount collected from the customer shall be acknowledged by issuing a receipt (printed or electronic) on behalf of the Bank.

f. Bank shall be responsible for addressing all customer service aspects related to ATM/CRM of the bank as well as it's agents.

g. Bank shall also display Frequently Asked Questions (FAQs) on their website / mobile app related to the ATMs/CRMs.

16. Standard Operating Procedure:

Bank shall issue comprehensive SOP for ATM/Recycler site maintenance, ATM/CRM operations, Cash replenishment, Decommissioning of Automated machines, Installation of ATMs/CRMs, handling of customer complaints/grievances, settlement & reconciliation etc. and FAQs from time to time.

17. Reference

a. RBI Circular no RBI/2021-22/84 DCM (RMMT) No.S153/11.01.01/2021-22 dated 10th August 2021 regarding Monitoring of Availability of Cash in ATMs.
b. RBI Circular no DCM (Plg.) No. S1117/10.25.007/2021-22; dated March 31, 2022-Cassette - Swaps in ATMs
c. RBI Circular no CM (Plg.)No.2968/10.25.007/2018-19 dated June 14, 2019-Security Measures for ATMs.
d. RBI Circular no DBR No.Leg.BC. 21/09.07.006/2015-16 dated July 1, 2015-Master Circular on Customer Service in banks.

e. RBI Circular no RBI/2017-18/206 DBS.CO.CSITE/BC/.5/31.01.015/2017-18 dated August 27, 2015 dated 21.06.2018 regarding Control Measures for ATMs.

f. RBI Advisory: 1/2021 dated April 10, 2021 regarding Man in the Middle (MiTM) Attacks in ATMs.

Chapter V

UPI (Unified Payment Interface)

1. Aim of this policy:

1.1. Introduction:

UPI is an instant payment system developed by NPCI. The Interface facilitates inter-bank peer to peer transactions. The UPI Policy, hereinafter referred to as the "Policy", is aimed at providing guidance to the employees and customers of Bank of Maharashtra (hereinafter called the "Bank"), and to lay down the systems and controls expected for managing the UPI onboarding.

The policy documents govern the current business strategy of the Bank with regard to onboarding of its esteemed customers on UPI Channel. The policy also lays out the various charges and terms associated with UPI usage.

1.2. Governance and Intended Audience:

This policy is intended for the concerned departments within the Bank, who are dealing with products where UPI onboarding is done. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank and also of various regulators, including the Reserve Bank of India.

The DBD & IT Department shall be responsible for maintaining the infrastructure related to UPI onboarding and shall work with the concerned departments to ensure that features proposed to the customers are implemented correctly within the various systems of the Bank.

1.3. Important Specifications of a UPI:

a. **UPI:**

i. The Unified Payment Interface (UPI) is a technology that combines multiple banking services, smooth fund routing and merchant payments into a single mobile app that can be used by any bank that participates. It also works "Peer- To – Peer" requests, which can be scheduled and paid for based on need and convenience.
ii. Immediate money transfers through mobile device round the clock 24*7 and 365 days. Single Mobile Application for accessing different Bank Accounts. It facilitates push(pay) and pull(receive) transactions and even works for the over the counter or QR based barcode payments as well as multiple recurring payments such as utility bill and other subscriptions.
iii. Virtual Address of the customer for Pull and Push provides for incremental security with the customer not required to enter the details such as Card No, Account No, IFSC etc.

b. **Understanding UPI:**

i. "UPI Application" shall mean the Bank's Unified Payments Interface Application downloaded by the user to his/her mobile phone from authorized source.

ii. NPCI" shall mean National Payments Corporation of India, a company incorporated in India under Section 25 of the Companies Act, 1956 and having its registered office at 1001A, B wing 10th Floor, The Capital, Plot 70, Block G, Bandra- Kurla Complex, Bandra (East), Mumbai - 400 051, and acting as the settlement, clearing house, regulating agency for UPI services with the core objective of consolidating and integrating the multiple payment systems with varying service levels into nation-wide uniform and standard business process for all retail payment systems.

iii. **"UPI Services"** shall mean Unified Payments Interface, a multi-platform operable payment network solution which is being provided by NPCI for the purpose of inter-bank transfer of funds i.e., pay someone (push) or collect from someone (pull) pursuant to the rules, regulations and guidelines issued by NPCI, Reserve Bank of India and the Bank, from time to time;

iv. **"Payment Service Provider or PSP"** shall mean entities which are allowed to issue virtual addresses to the Users and provide payment (credit/debit) services to individuals or entities and regulated by the Reserve Bank of India, in accordance with the Payments and Settlement Systems Act, 2007.

v. **"User"** shall mean an individual / entity who is a holder of a Bank account who has downloaded Bank's UPI application, wishes to register with Bank's UPI application by accepting the terms and conditions and avails the UPI Facility

vi. **"Virtual Payment address (VPA)"**– is a payment identifier for sending/collecting money. VPAs are aliases to Account No. & IFSC. This enables the user to complete a transaction without having to enter the account credentials of the beneficiary.

vii. **"User's Mobile Number"** shall mean the specific mobile phone number registered by the user with Bank(s) where he / she is holding the accounts and that has been used by the User to register for the UPI Facility.

viii. **"Registration"** The User agrees that he/she shall be entitled to use the UPI Service by downloading Bank's UPI application provided that /his/her Mobile Phone is found inorder to technologically support the UPI application and the relevant particulars are registered with the Bank.

ix. **"AADHAR Number"** Shall mean the Unique Identification Number issued by Unique Identification Authority of India (UIDAI).

x. **"MPIN"** Shall mean the Mobile Personal Identification Number created by the user for authenticating the services provided under UPI.

xi. **"Account"** shall mean Savings and/or Current/Overdraft account held in individual capacity at present at the bank which has been enabled for UPI. The term "Accounts" also including Prepaid Instrument accounts i.e. wallet accounts.

xii. **"Merchant"** shall mean a merchant established under the prevalent law and has an agreement with Master Merchant to accept payment through UPI Services towards the sale of products or services to its customers.

xiii. **"Remitter Bank"** shall mean a bank holding a bank account of the Payer where the Debit of the UPI instruction is received from the Payer to be executed on real time basis.

xiv. **"Beneficiary Bank"** shall mean the Bank holding a bank account of the Receiver where the credit of the UPI instruction is received from the Payer to be executed either in real time basis or periodically with a settlement process.

xv. **"Authentication Credentials"** shall mean password, biometrics, PIN etc., as created by the user or provided by the Bank from time to time, which shall be required by the Customer for completion of the transfer of funds through UPI.

xvi. **"Authorization/Authorized Transactions"** means the process by which Bank approves a Transaction as stipulated by competent authorities/ 3rd parties, from time to time.

xvii. **"Chargeback"** shall mean approved and settled UPI transactions which are at any time refused, debited or charged back to Merchant's account by the Issuer, Acquiring Bank or NPCI for any reason whatsoever, together with Bank fees, penalties and other charges incidental thereto.

xviii. **"Customers"** shall be used to collectively refer to Payer(s) and Receiver(s) using UPI services on Merchant Platform for initiating and executing UPI transactions.

xix. **"Receiver"** shall mean any person or the Merchant holding a banking account, who are desirous to receive payments from the Payer over the internet using the UPI Services. In case the Payer is customer of the Merchant and is paying money to the Merchant for purchase or utilization of goods and services from the Merchant, the Merchant shall be the Receiver.

xx. **"MMID"** Mobile Money Identifier(MMID) is a seven digits random Number issued by the Bank upon registration. Remitter (Customer who wants to send money) and Beneficiary (customer who wants to receive the money) should have this MMID for these interbank funds Transfer.

xxi. **"Payer"** shall mean any person holding a banking account and who desires to pay money to the Receiver for purchase of goods or services online using the UPI Services, being offered by the Merchant on its website or mobile application thereto.

xxii. **"Amount"** shall mean the payment amount in question which is required to be transferred from the Payer to the Receiver via the Merchant as a part of the UPI Transaction.

xxiii. **"Service Providers"** means banks, financial institutions and software providers who are in the business of providing information technology services, including but not limited to, internet based electronic commerce, internet payment gateway and electronic software distribution services and who have an arrangement with Bank or with NPCI to enable use of UPI Software developed by them to route UPI Transactions.

xxiv. **"Merchant Account"** shall mean Bank account of the Merchant maintained with Bank for collecting Fees, charges and other levies. In case the Merchant intends to use this Merchant Account to settle UPI transactions, for which the Merchant is the Receiver, then the Merchant Account shall also be used for settlement of transactions using UPI Services.

xxv. **"Transaction"** shall mean every payment instruction that results in a debit to the Payer's Account and a corresponding credit to the Receiver's Account.

xxvi. **"Commission"** means the commission, fees, charges or levies payable to the Bank, for facilitating a Transaction.

xxvii. **"Merchant Platform"** shall mean the website/mobile with the domain name or Application name and which is established by the Merchant Platform for the purposes of enabling Payers and Receivers to carry out Transactions.

c. **Personal Identification Number (PIN):**

PIN is a 4 Digit passcode which a user need to set while registering on an UPI app for the first time. It's a very important passcode number which is required for all

payment transactions. A user must remember their UPI PIN and importantly not to share with anyone. It is advised that the customer changes the PIN frequently. This may be carried out by using SET/Reset PIN functionality in the UPI application prescribed by the Bank.

d. **Types of transactions supported by UPI:**

i. Financial transactions

UPI supports the following financial transactions:

Pay/Push Request:

A transaction where the initiating customer 'pushes' funds to the intended beneficiary. Payment address includes mobile number and MMID, account number with IFSC, and Virtual ID.
User Logs into the UPI Application. After Successful login user selects the option of Send Money/Payment. Users enters beneficiary's/Payee Virtual Id, Amount and selects the amount to be debited.
User gets confirmation screen to review the payment details and click on confirm and enters the PIN to send/Pay the money.

Collect/Pull Request:

A transaction where the customer is 'pulling' funds from the intended remitter by using a Virtual ID. User Logs into the UPI Application. After Successful login user selects the option of collect money (request for Payment) in Collect/Pending Requests and enters remitter's/Payers Virtual ID, Amount and selects the amount to be credited
User gets confirmation screen to review the payment details. The Payer gets notification on his mobile for request money. Payer then decided\s to accept or decline. In case of Payment payer enters the PIN to authorize the transaction and Payee gets notification from bank for credit of his Bank Account.

Scan & Pay Request:

A transaction where the customer 'pushes' to merchant outlet by simply scanning QR Code funds from the intended remitter by using Bank's UPI application.

ii. Non-financial transactions

UPI will support the following types of non-financial transactions on any PSP app.

Deregistration for UPI banking: Customer can de register for Bank's UPI application by submitting the Deregistration request and MPIN.

Balance Enquiry: - Customer can check for Balance of account which is linked for UPI for Bank's UPI Application by entering TPIN.

Set/change PIN: For New User Customer has to go to existing Bank of Maharashtra Customer and select Register option. Thereafter Enter CIF/Account No customer can set for set UPI PIN Customer can set new PIN using Aadhaar OTP or Debit Card. Change UPI ID by using Aadhaar OTP or Debit Card. For availing Aadhaar OTP functionality, Customer's Mobile No should be registered with UIDAI so as to receive OTP from UIDAI.

UPI Mandate: The Customer can set any mandate for making recurring payment using this functionality.

Transaction Status Check: The Customer can check the status(Success/Failure) for earlier made payment using this functionality.

Add/Manage Payee/Beneficiaries: The Customer can add beneficiary for making payments without need to reenter beneficiary details (mobile number and MMID, account number with IFSC, and Virtual ID) each time.
Manage Blocked UPI ID:- The Customer can Block/ Unblock any Person/Merchant using this functionality

Share QR:- This Functionality is present in (MY QR Code→Static & Dynamic QR for doing Collect Request where customer shares the Dynamic/Static QR Code to remitter to receive money. In Static QR Code the Customer only share the QR Code to remitter where remitter scans the QR Code and enters the amount manually to send the money. While in Dynamic QR Code the Customer generates the QR Code with the amount (which he wants to receive) to remitter, The Remitter scans the QR and only needs to authorize the payment to remit the amount (already set by the customer while sending QR Code).

Raising disputes/queries: The disputes/queries can be raised in the application mentioning the details of the transaction. UDIR shall be used for raising of complaints/disputes for resolution and check dispute status through payer App. UDIR provisions as per RBI circular dated 06/08/2020 & NPCI OC 98 dated 20/11/2020 shall be adhered.

*UPI registration is only possible if the mobile number (which is to be registered) is already registered with the issuer bank for SMS /mobile alerts. UPI can be accessed on all major platforms such as Android and iOS with apps developed by members. Bank issues various types of personalized and non-personalized debit cards.

e. **UPI Fees**:

At present there are no charges levied on transactions done via UPI. The government has mandated a zero-charge framework till now. This means that charges in UPI were nil for users and merchants alike. However, since April 1, 2023 merchant transactions exceeding Rs. 2,000/- in value done using Prepaid Payment Instrument Wallets (PPI Wallets) on UPI will attract an interchange charges of 1.1%.

The Bank shall decide the fees and charges as and when required related to onboarding for UPI Services considering NPCI directives and approval from competent authority. The same shall be facilitated by the planning department with recommendation of digital banking department.

2. Services Available on UPI:

a. At Bank's Application:

i. Push Request (Send Money)
ii. Pull Request (Collect Money)
iii. Set/Change PIN
iv. Transaction status check
v. Balance Enquiry
vi. Mini Statement
vii. Change of PIN
viii. Standing Instructions (SI),

ix. Mandate Registration,
x. ASBA

b. At Other PSP:

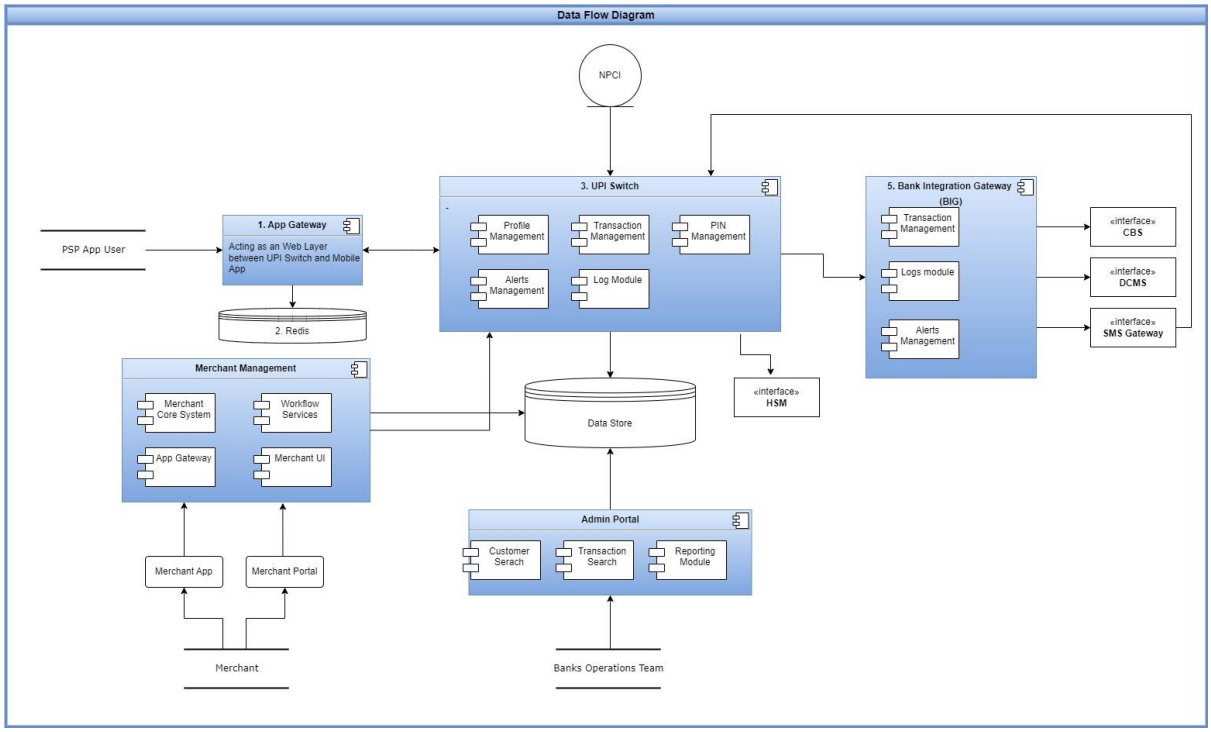
i. Push Request (Send Money)
ii. Pull Request (Collect Money)
iii. Balance Enquiry
iv. De-register/Remove Account

c. For online usage:

For online purchase, ticket booking (Railway, Movie, Bus etc.), payment of Bills etc. customer can use UPI Collect / QR Scan.

d. New services will be added as per the prevailing guidelines after approval from the competent authority. Bank shall comply & implement the notifications/ guidelines from RBI /NPCI vide OCs & other regulatory guidelines issued by GOI as per applicability.

3. Digital Payment Cycle:



4. Compliance with Other instructions

In consideration of Bank providing these facilities, the User agrees to indemnify and hold the Bank, its directors & employees, representatives, agents & its affiliates harmless against all actions, suits, claims, demands proceedings, loss, damages, costs (including attorney fees), charges and expenses which the Bank may at any time incur, sustain, suffer or be put to as a consequence of or arising out of or in connection with any services provided to the User pursuant hereto. The User shall indemnify the Bank, its directors & employees, representatives, agents & its affiliates for unauthorized access by any third party to any information / instructions / triggers given/received by the User or breach of confidentiality.

5. Operation of Pre-Sanctioned Credit Lines at Banks through Unified Payments Interface (UPI)

a. Currently, savings account, overdraft account, prepaid wallets and credit cards can be linked to UPI. Under this facility, payments through a pre-sanctioned credit line issued by a Bank to individuals, with prior consent of the individual customer, are enabled for transactions using the UPI System.

Banks may, as per their Board approved policy, stipulate terms and conditions of use of such credit lines. The terms may include, among other items, credit limit, period of credit, rate of interest, etc.

6. Customer Service Policy

a. Bank shall put in place a Grievance Redressal Mechanism within the card issuing entity and give wide publicity about it through electronic and print media. Incharge Customer Service Department shall ensure that grievances of on boarded UPI Customer are redressed promptly without any delay. Specific timelines may be stipulated in the Board approved policy for Redressal of grievances and compensation framework. The grievance Redressal procedure and the Board approved policy shall be displayed on the website of the Bank with a clearly visible link on the homepage.

b. Bank shall ensure that the call center staff are trained adequately to competently handle and escalate, a complaint, if necessary. The Grievance Redressal process shall have a provision for automatic escalation of unresolved complaints from a call center/base level to higher authorities. There shall be a system of acknowledging customers' complaints for follow up, such as complaint number/docket number, even if the complaints are received over phone.

c. Bank shall be liable to compensate the complainant for the loss of his/her time, expenses, financial loss as well as for the harassment and mental anguish suffered by him/her for the fault of the card-issuer and where the grievance has not been redressed in time. If a complainant does not get satisfactory response from the card-issuer within a maximum period of one month from the date of lodging the complaint, he/she will have the option to approach the Office of the concerned RBI Ombudsman for Redressal of his/her grievance/s. Timeline (TAT) for escalation of complaints, level of escalation and other details pertaining to grievances and compensation shall be governed by Bank’s Customer Service Policy.

7. Compliance

Compliance with Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation under the PMLA, 2002

The instructions/Directions on KYC/AML/CFT issued by RBI and Bank from time to time, shall be strictly adhered to in respect of all cards issued, including co-branded cards.

8. Handling of Customer Complaints/ grievances:

a. Customer should lodge representation/ queries/ complaints, either at the home branch or at the Mahaseva. The UPI on-boarding is issued on the condition that the bank bears no liability for unauthorized use of UPI. Customer shall be aware of any kind of

information being shared with any other organization and type of information being shared to avoid any conflicts on part of the Bank.

In cases where the loss is due to negligence by a customer, such as where he has shared the authentication 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.

b. Any person other than the UPI on boarded customer can gain unauthorized access to the UPI services if he/ she gains possession of the Mobile & PINs (MPIN/TPIN). The card is issued on the condition that the bank bears no liability for unauthorized use of the UPI. The responsibility is fully that of the card holder. On receipt of any complaint from customer, the same is to be attended by the respective branches promptly and grievances should be redressed within time limit prescribed by NPCI. Complaints could of the following nature:

Nature of Complaint	Handling Mechanism
Mobile lost / stolen / damaged	Branch / customer should contact Mahaseva through toll free number / email and block the UPI Channel.
Amount debited from account but money not dispensed	Complaints pertaining to our banks customers should be accepted in the prescribed format at Branches. Other bank customers should be advised to route their complaint through their UPI Issuer bank through DCMS Portal.
Partial amount dispensed	Complaints pertaining to Bank customers to be accepted through prescribed format at Branch, other bank customers to be advised to route their complaint through their UPI Issuer bank through DCMS Portal.
Disputes regarding operations / service charges	Branch / Bank's Customer Care / Call Centre will handle such complaint.

Bank shall ensure timeline for reconciliation as per RBI guidelines on Harmonization of TAT for UPI. Timeline, Grievance Redressal procedure, Name, address and contact number of the important executives as well as Grievance Redressal officer of the bank etc. for resolution of grievances is given under Bank's Grievance Redressal policy. The said information is available on Bank's website and also periodically reviewed/changed.

9. Unsolicited commercial communication:

Bank may ensure that they engage telemarketers who comply with directions/ regulations issued by the Telecom Regulatory Authority of India (TRAI) from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)" and "Measures to curb misuse of Headers and Content Templates under Telecom Commercial Communications Customer Preference Regulations, 2018".

10. Lost or stolen Mobile reporting by customer:

a. If any Customer's Mobile is lost or stolen or if PIN is disclosed to a third party, customer should report the incident immediately by calling Mahaseva or by sending e-mail to mahaconnect@mahabank.co.in.

b. Customer is liable for all amounts debited to account using UPI Services as a result of the unauthorized use of card/ PIN until reported loss, theft or disclosure of your card or PIN.

11. Indemnity:

In consideration of Bank providing these facilities, the User agrees to indemnify and hold the Bank, its directors & employees, representatives, agents & its affiliates harmless against all actions, suits, claims, demands proceedings, loss, damages, costs (including attorney fees), charges and expenses which the Bank may at any time incur, sustain, suffer or be put to as a consequence of or arising out of or in connection with any services provided to the User pursuant hereto. The User shall indemnify the Bank, its directors & employees, representatives, agents & its affiliates for unauthorized access by any third party to any information/instructions/triggers given/received by the User or breach of confidentiality.

12. Standard Operating Procedure:

Bank shall issue comprehensive SOP for on-boarding of customer for UPI services, on-boarding of customer for UPI services for multiple Banks, De-registration of UPI services, Financial transactions, settlement & reconciliation, Usage Policy, Termination of UPI Service for User, Terms and conditions for UPI to customers, Liability for the User, Liability of Bank, General Conditions, Escalation Matrixetc. and FAQs from time to time.

Chapter VI

QR CODE (Quick Response Code)

1. Preamble

The Digital India program is flagship program of government of India with vision to transform India into digitally empowered society and knowledge economy. The main preamble for QR code orientation is to protect the merchant data. The Reserve Bank of India released guidelines to make QR code interoperable to help the electronic payment ecosystem achieve scale. RBI has advised vide letter no. RBI/2020-21/59 DPSS.CO. PD. No.497/02.14.003/2020-21 for formulation of Bank's own digital payment channel policy by streamlining QR code Infrastructure. The main objective for Bank QR code implementation is to enhancing shopping experience of buyers.

2. Purpose

QR code can provide end to end encryption security feature for banking or any financial institutions and to its customer to carry out secure transactions. Any Merchant who is performing business through account can avail the QR code for business account and can share the QR code to other people to quickly transfer money. This QR code policy documents enables financial institutions to secured payments, brand enhancement and multi-level authentications. This QR code policy documents is guiding principles in respect of on boarding merchants for QR codes, transactions by using QR code scanner, settlement and dispute resolution. The policy shall be guided by Payment & Settlement systems act 2007. The National Payments Corporation of India (NPCI) is an umbrella organization that operates retail payments and settlement systems in India.

3. Stakeholders in Merchant Acquisition Business

The main stakeholders in the QR code Business are as under:

a. **Issuer**: QR code issuing institution/ issue bank

b. **Remitter/Payer**: Customer who is transferring money by scanning QR code of merchant from any UPI linked Mobile App.

c. **Beneficiary/ Payee**: Entity which accepts payment through QR code or any other digital channel.

d. **Beneficiary Bank**: The bank that accept the payment of merchant in respective accounts from his customers.

e. **Issuing Bank**: The Bank provides necessary infrastructure or issuing QR code to the merchant to accept payment, maintain relationship and facilitate acceptance of payments through scanning of QR code.

f. **NPCI**: NPCI provides online transaction routing, processing and settlement services to members participating in UPI.

g. **MCC code:** classification of merchant according to business turnover and business type.

h. **Regulator**: RBI as a regulator of electronic payments in India.

4. QR code payment Functioning

QR codes generally create a sort of pixel pattern with each part containing a piece of Iinformation.it is two dimensional barcode that can be scanned by smartphone or other mobile devices linked with UPI. In the case of digital payments, the information can be, merchants' details, transaction details, etc. Upon scanning, QR code patterns (horizontal and vertical black patterns on white background) get decoded by the software and get converted into the character string. The QR codes (for payment acceptance) generally carry commands related to transactions.

Merchant can generate QR codes for his shop, or for any fixed or variable amount. According to this command, the QR code is generated. It either opens a payment link, confirms payment, or does any other operation as specified. The customer just has to scan it and then transfer payment.

5. Merchant On-boarding Process for QR code and usage

QR code payment is a contactless payment method where payment is performed by scanning a QR code from a mobile app. UPI transaction limit per day is Rs.1 lakh as per NPCI.

To scan QR code customer will need:

- A barcode reader/ QR scanner.
- A smartphone with an inbuilt camera.
- (Nowadays, there are many apps with which, QR codes can be scanned with utmost ease)

Using a smartphone for scanning the QR code displayed on the shop's checkout, products, website, etc. and making online payments. Customer can just scan the QR Code, provided by the merchant, using smartphone (customer phone must have a camera). Not only do QR codes facilitate instant payment, but online payment can also be extremely quick compared to other methods. A customer just has to open the QR code application to scan the code and pay.

After confirming the payment processing, payment is done within a few seconds. Setting up QR code payments is extremely easy. There is no need for any additional overhead cost or infrastructure to set up a QR code. QR codes can be simply printed on paper and can be used for scanning and payment.

Merchant don't need much of an infrastructure. Payment acceptance via QR code also eliminates the requirement of any third-party application or physical device like POS.

QR code payments are a fool proof payment method as it eliminates the probability of any kind of error. The pattern of black boxes consists of unique data which enhances the reliability of the QR code payments.

Digital Banking Department shall perform assessment of usage of issued QR on yearly basis considering uptime of number transactions per QR, amount of transactions per QR, frequency of usage of QR, etc.

6. Types of QR Code

There are two types of categories for QR codes:

a. Static QR code:

i. Static QR code contains the Payment URL directly placed inside. As these QR codes are static, the content of the codes cannot be altered and these codes also cannot be tracked.
ii. They are used for quick and simple online payment acceptance. Customers just have to scan the QR code, enter the purchase amount, the merchant will verify the details and then the customer can initiate the online payment.
iii. We often come across such codes at small shops, at restaurants, hardware stores, medicals, in-store retails, etc.

b. Dynamic QR code:

Dynamic QR codes send users on to specific information or web pages, just like any other QR code. What makes them "dynamic" is that the URL encoded in them redirects to a second URL that can be changed on demand, even after a code is printed. Static QR codes can't be changed in that way.

Dynamic QR code is editable QR code. Merchant can generate QR code for specific amount of payment acceptance.

7. Merchant Category code (MCC Codes)

Merchant Category Codes (MCCs) are four-digit numbers that describe merchant's primary business activity. NPCI assigns the Merchant Category to respective merchants according to their business type or goods and services provided.

8. Merchant On-boarding

a) Merchant Self on-boarding:

Merchant can do self on-boarding by using Maha Merchant mobile application and can generate static or dynamic QR code. Application is available with Google Play store.

b) *Web portal for Branches*:

This portal is applicable for both small and corporate merchants. Branches can issue QR code to merchant by using Portal with proper merchant categorization.

Note: Branches are required to do due-diligence while selection of merchant. It is branch responsibility to identify merchant according to their business volume and on board for QR code.

9. Deactivate QR Codes

Bank shall ensure deactivation of QR codes/merchant ID not having any financial or non-financial transaction in last one year.

10. Standard Operating Procedure:

Bank shall issue comprehensive SOP for operation of QR code and FAQs from time to time.

11. References

a. Reserve Bank of India guideline for “Digital Payment Transactions – Streamlining QR Code infrastructure” Circular No: RBI/2020-21 / 59DPSS.CO.PD.No. 497/02.14.003 / 2020-21 dated 22 Oct 2020.
b. Payment Regulation and supervision of payment system is as per “The Payment And Settlement Systems Act, 2007” of RBI.
c. Operation of Pre-Sanctioned Credit Lines at Banks through Unified Payments Interface (UPI) RBI/2023-24/58 CO.DPSS.POLC.No.S- 567/02-23-001/2023-2024
d. Mandatory measures to be implemented by the NPCI/UPI/OC 168/2023-24 dated 4th July 2023

Chapter VII

WhatsApp Banking

1. Aim of this policy:

1.1. Introduction:

The WhatsApp Banking Policy, hereinafter referred to as the "WAB Policy", is aimed at providing guidance to the employees and customers of Bank of Maharashtra (hereinafter called the "Bank"), and to manage the systems expected for governing the WhatsApp Banking.

The policy aims at the current business strategy of the Bank with regard to issuance of WhatsApp Banking to its esteemed customers. The policy also lays out the various charges and terms associated with WhatsApp Banking.

1.2. Governance and Intended Audience:

This policy is designed for the concerned departments/Branches within the Bank, who are dealing with products where WhatsApp Banking issuance is required. The Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank and WhatsApp (Meta).

The DBD Department shall be responsible for maintaining & enhancement of WhatsApp Banking.

2. Important Specifications of WhatsApp Banking:

2.1 WhatsApp Banking:

i. Bank has introduced "WhatsApp Banking" services as an additional service delivery channel towards convenience for the customers. The services can also be availed by Bank's non-customers. Send "Hi" to 70660 36640 to interact with WhatsApp Banking.

ii. Bank can power its customer services delivery with real-time Account Balance enquiry, Mini-Statement, Loan Account Enquiry, Account Statement, Pension Slip, Cheque book request, enquiry of cheque status, locate Bank's ATMs and Branches, Opt-In, Opt-Out, Contact us information etc.

2.2 Salient features of WhatsApp Banking:

i. Banking services anytime anywhere 24X7
ii. Free of cost service to the customer
iii. Secured service with end to end encryption
iv. Customer can receive alerts, messages, notifications, offers, updates directly from Bank
v. Easy Opt-in/Opt-out mechanism

2.3 Fees

WhatsApp Banking is free of cost service to the customer excluding internet charges of service provider.

3. Services Available in WhatsApp Banking:

1) Know your Account Balance
2) Know Customer ID / CIF
3) Get Mini Statement
4) Get Account Statement (For last 3 Months)
5) Loan Account Balance Enquiry
6) Get information about nearby Bank's ATM or branch
7) Cheque Book Request
8) Cheque Book Status
9) Opt-In / Opt-Out
10) Contact Us

Any addition /deletion/enhancement in services shall be done after approval of CDO/GM digital banking and shall be put up to ORMC on quarterly basis.

4. Usage Policy:

The WhatsApp Banking shall be governed by the below terms and conditions:

These terms and conditions ("WhatsApp Terms and Conditions" as amended from time to time) are applicable to the Customers (defined hereinafter) who avail the Services (defined hereinafter) provided thereon by Bank of Maharashtra ("Bank") on the WhatsApp platform and who are eligible for certain select banking services. The WhatsApp Terms and Conditions shall be in addition to any other terms and conditions as stipulated by the Bank from time to time on its website (https://bankofmaharashtra.in/whatsapp-banking) whether pertaining to the account or in relation to other products, services, facilities or offers provided by the Bank. Any services that may be offered to the customer through the WhatsApp platform ("WhatsApp") is at the discretion of the Bank and/or basis the eligibility criteria of a customer and such services are subject to certain terms and conditions. Further, in case of inconsistency between the WhatsApp Terms and Conditions and any specific terms and conditions pertaining to a specific variant of the account or any specific service/product/offer, the specific terms and conditions of that particular service/product/offer shall prevail.

5. Customer Eligibility for WhatsApp Banking use:

User needs to have account in Bank. To activate the banking facility on WhatsApp, customers need to save Bank of Maharashtra WhatsApp Number **70660 36640** in their phone's contact list. Customer to send message e.g. "Hi" to interact with the Bank's WhatsApp solution.

5.1. Bank Customers:

The Customer hereby agrees and undertakes that he/she shall use the Services only if he/she fulfils the eligibility as given below: -

i. The Customer is a resident of India and is present in the territory of India at the time of utilization of the Services
ii. The Customer is a non-resident India (NRI) or is residing outside India.
iii. The Customer has registered its Mobile Number with the Bank.
iv. The customers having a satisfactory running Savings/ Current/ Over Draft/ Cash Credit account with the Bank.

5.2. **Non-Bank Customers:**

Non-Customers will be provided limited services such as instant account opening link, locate branch/ATM etc.

6. General Conditions:

a. These WhatsApp Terms and Conditions form a contract between the Customer and Bank. The Customer shall apply to Bank in the prescribed manner for availing of the Services.
b. By applying and opting in for the Services, the Customer acknowledges that he has read, understood and accepted these WhatsApp Terms and Conditions and other specific terms and conditions as may be pertaining to the Account and any other products/offers/facilities and services availed by the Customer whether or not through WhatsApp.
c. No act, delay or omission by the Bank shall affect its rights, powers and remedies under these Terms and Conditions and other terms on the Bank website (https://bankofmaharashtra.in/whatsapp-banking), hereinafter referred to as "Website".
d. The Customer hereby accepts and agrees that all Services and communications (both One Way Communication and Two Way Communication) taking place on WhatsApp, initiated either by the Bank or the Customer, will be governed by and subject to these WhatsApp Terms and Conditions.
e. Further, the Customer hereby agrees that the Customer grants express authority to the Bank for carrying out the Services requested by the Customer on WhatsApp on its Registered Bank Number.
f. Provided however that the Bank shall not be required to authenticate the Customer, if any request for the Services comes on WhatsApp to the Bank Registered Number, and in case of a Customer, if the number reflected in the requestor's mobile is a Customer's Registered Number, the Bank shall be entitled to presume that it is the Customer itself which is interacting through WhatsApp and in case of non-Customer the Bank shall be entitled to presume that the number reflected in the WhatsApp profile is the said non Customer's number and it is the said non Customer itself and not any other person who is interacting with the Bank Registered Number.
g. The Bank's own record or log of transactions maintained through computer systems or otherwise shall be accepted as conclusive and binding for all purposes.

7. Unsolicited commercial communication:

Bank may ensure that they engage telemarketers who comply with directions/ regulations issued by the Telecom Regulatory Authority of India (TRAI) from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)".

8. Disclaimer of liability:

Bank shall not be responsible for any failure on the part of the Customer to utilize the WhatsApp facility due to the Customer not being within the geographical range within which the WhatsApp facility is offered and which forms part of the roaming network of such cellular service provider, providing services to the Customer availing such roaming facility from the respective cellular service provider. If the customer has reason to believe that the mobile phone number is / has been allotted to another person and / or there has been an

unauthorized transaction in the account and / or his mobile phone handset is lost, he shall immediately inform Bank of the same. The Customer agrees that Bank shall not be liable if:

a. The Customer has breached any of the terms and conditions, contained herein or
b. The Customer has contributed to or the loss is a result of failure on part of the Customer to advise Bank within a reasonable time about unauthorized access of or erroneous transactions by use of the Services; oars a result of failure on part of the Customer to advise Bank of a change in or termination of the Customer's mobile phone numbers/SIM (“Subscriber Identity Module”) cards. Any unauthorized use of the customer's OTP/debit card PIN, password or mobile phone number or for any fraudulent, duplicate or erroneous instructions given on the WhatsApp channel;

c. There has been an unauthorized transaction/instruction provided through the WhatsApp channel as a result of any person having control or custody of telecommunications instrument (such as the mobile handset) so that such instrument may be used to give telecommunications instruction without authorization or any other issue/default/error/technological problem in the telecommunication instrument (such as the mobile handset) or duplication of mobile number / SIM of the Customer such as but not limited to SIM card cloning, virus in handset etc.
d. Acting in good faith on any instructions received by Bank from or on behalf of the Customer in relation to the WhatsApp facility
e. Error, default, delay or inability of Bank to act on all or any of the instructions given by the Customer due to any reason;
f. Unauthorized access by any other person to any information /instructions given by the Customer or breach of confidentiality
g. Bank makes no representation or gives no warranty with respect to the quality of the service provided by any cellular service provider or by WhatsApp or any other service provider enabling Bank to deliver services through WhatsApp to the Customers.
h. Bank may provide any other services as a part of the WhatsApp facility and Bank shall not be liable for the oversight on part of the Customer to update himself /herself with the addition of services which have been included in the WhatsApp facility.

9. Standard Operating Procedure:

Bank shall issue comprehensive SOP for Understanding WhatsApp Banking, steps to follow for WhatsApp Banking, Inactivation of WhatsApp Banking, operations of WhatsApp Banking Redressal of grievances, escalation of unresolved complaints, Handling of customer complaints/grievances. and FAQs from time to time.

Chapter VIII

Digital Signature

1. Aim of this policy:

1.1. Introduction:

The Digital Signature Policy, hereinafter referred to as the “Policy”, is aimed at providing guidance to the employees of Bank of Maharashtra (hereinafter called the “Bank”), and to lay down the systems and controls expected for managing the Digital signature system.

The policy documents govern the current business strategy of the Bank with regard to issuance of Digital signature to its employees and other required entities. The policy also lays out the various charges and terms associated with Digital signature usage.

1.2. Governance and Intended Audience:

This policy is intended for the concerned departments within the Bank, who are dealing with products where Digital signature is used. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank and also of various regulators, including the Reserve Bank of India.

The Digital Banking Department shall oversee the Digital signature issuance to various Branches/zones. IT Department shall do the procurement as per business requirement.

2. Important Specifications of a Digital signature:

2.1. Digital signature:

i. "**Digital Signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of IT Act

ii. “**Digital Signature Certificate Applicant” or “DSC Applicant**” —A person that requests the issuance of a Digital Signature Certificate by a Certifying Authority.

iii. “**Digital Signature Certificate Application” or “DSC Application**” —A request from a Digital Signature Certificate applicant to a CA (Certifying Authority) for the issuance of a Digital Signature Certificate issued under subsection (4) of section 35 of the Information Technology Act, 2000.

iv. “**ESP” or “eSign Service Provider”** is a Trusted Third Party to provide eSign service. ESP is operated within CA Infrastructure & empaneled by CCA (Controller of Certifying Authority) to provide Online Electronic Signature Service.

2.2. Understanding a Digital Signature:

i. “**Private Key"** means the key of a key pair used to create a digital signature

ii. **"Public Key"** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

iii. **"Registration Authority" or "RA"** is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of applicant's credentials

iv. **Subscriber**— A person in whose name the Digital Signature Certificate is issued by CA.

v. **Time Stamping Service:** A service provided by CA to its subscribers to indicate the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

2.3. Types of Digital Signatures:

The following table provides an overview of the different types of Digital Signature Certificates.

i. Individual Digital Signature Certificates (Signing Certificates)

Individual Certificates serve to identify a person. It follows that the contents of this type of certificate include the full name and personal particulars of an individual. These certificates can be used for signing electronic documents and emails and implementing enhanced access control mechanisms for sensitive or valuable information. These certificates are applicable for the Bank employees.

ii. Server Certificates

Server Certificates identify a server (computer). Hence, instead of a name of a person, server certificates contain the host name e.g. **"https://nsdg.gov.in/ "** or the IP address. Server certificates are used for 1 way or 2 way SSL to ensure secure communication of data over the network.

iii. Encryption Certificates

Encryption Certificates are used to encrypt the message. The Encryption Certificates use the Public Key of the recipient to encrypt the data so as to ensure data confidentiality during transmission of the message. Separate certificates for signatures and for encryption are available from different CAs.

2.4. Digital signature Fees:

i. **Certificate Issuance and Renewal Fees:** The fees for various types of certificates are made available on CA website at https://idrbtca.org.in/ and will be updated from time to time.

ii. **Certificate Access Fees**: CA is not charging any fees to relying parties or other public for accessing the certificate information from the repository. The certificate search facility is provided free of cost at its website https://idrbtca.org.in/

iii. **Revocation Status Information Access Fees:** CA does not charge a fee for access to any revocation status information. CA may charge a fee for providing certificate status information.

iv. **Fees for Other Services**: No stipulation

v. **Refund Policy**: The refund policy and other payments terms are governed as per the terms in the subscriber agreement. In case the application is rejected the full amount would be refunded to the subscriber.

3. Usage Policy:

The Digital Signature usage policy is as under:

i. System Certificates:

The Subject Name MUST contain either IP Address of the system as a printable string in "network byte order", as specified in [RFC791] or MAC Address of primary network interface as a printable string or Serial number (CPU or any electronically verifiable serial number) as a printable string or Unique ID (such as CPU identifier) as a printable string.

ii. Time stamping authority certificate:

Licensed CAs my issue certificates for the purpose of time stamping. It should follow same naming conventions as a CA with “CA” and “Certifying Authority” replaced with “TSA” and “Time Stamping Authority” respectively.

4. Legal Validity of Digital Signatures:

a. The Indian Information Technology Act 2000 (http://www.mit.gov.in/content/information-technology-act) came into effect from October 17, 2000.

b. One of the primary objectives of the Information Technology Act of 2000 was to promote the use of Digital Signatures for authentication in e-commerce & e-Governance. Towards facilitating this, the office of Controller of Certifying Authorities (CCA) was set up in 2000.

c. The CCA licenses Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000.

d. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time.

e. The Root Certifying Authority of India (RCAI) was set up by the CCA issues Public Key Certificates to the licensed CAs and these licensed CAs in turn issue DSCs to end users.

f. Section 5 of the Act gives legal recognition to digital signatures based on asymmetric cryptosystems.

g. The digital signatures are now accepted at par with the handwritten signatures and the electronic documents that have been digitally signed are treated at par with the paper based documents.

h. An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include other techniques for signing electronic records as and when technology becomes available.

5. General Conditions:

5.1 The Subscriber should provide the correct, trustworthy, accurate, current and complete information to CA and/or its authorized Registration Authority (RA).

5.2 The Subscriber consents to third-party, independent verification of the information submitted by him and expresses his agreement to the terms and conditions of this Subscriber Agreement.

5.3 The Subscriber will promptly inform the CA if any of the information provided in the application is changed.

CA reserves the right to revoke the Subscriber's Digital Signature Certificate at any time, after having given the Subscriber an opportunity of being heard in the matter, in case it believes that the Subscriber's verified credentials have changed and / or his private key is compromised and / or he has breached the terms and conditions of this agreement

5.4 Under above circumstances, if the Subscriber wishes to obtain a new certificate, he will have to reapply on paid basis.

5.5 Digital Banking Department shall review the unused Digital Signatures and Digital Signature issued to retired/terminated/resigned employees to avoid misuse.

6. Terms and conditions:

a. By submitting an application for Digital Signature Certificate and agreeing to the terms and conditions mentioned, the Subscriber is requesting that CA may issue a Digital Signature Certificate to him.

b. By submitting the application for Digital Signature Certificate, the Subscriber is specifically agreeing to the provisions of CA Certification Practice Statement (CPS).

c. The Subscriber is also agreeing that his Digital Signature Certificate may be published via website and / or made available in the (Directory, and therefore all information that forms part of a Digital Signature Certificate may be available to Relying Parties and/or the general public. This will not be treated as a breach of confidentiality of the Subscriber's personal information.

d. The Subscriber also agrees that he will not use the Digital Signature Certificate for any purpose that will directly or indirectly compromise the nation's security and interest.

e. The Subscriber also agrees that he will submit his private key(s) (only if used for encryption) to law enforcement agencies under the directions of the CCA or courts of India

7. IDRBT CA:

a. The Digital Certificates are at their sole risk and strictly for lawful purposes and will not infringe a third party's right

b. The use of the private key and/or its associated Digital Certificate constitutes acceptance of the terms of the IDRBT CA CPS

c. Erroneous utilization of the Digital Certificates or violation to the practices specified in IDRBT CA CPS shall be liable to be proceeded against, both under the relevant civil and criminal laws, and shall be subject to punishment under the Information Technology Act, 2000 or/and any other relevant law/s of the land.
d. The duties of the subscribers to be followed are described in the Chapter VIII of The Information Technology Act, 2000.

e. The IDRBT CA disclaims all warranties, except as expressly provided in the IDRBT CA CPS. IDRBT CA makes no representations or warranties, express, implied or otherwise relating to IDRBT CA Digital Certificate or any services provided by IDRBT CA in connection therewith, including without limitation any warranty of non-infringement, merchantability or fitness for a particular purpose.

f. Bank shall ensure compliance of Gazette notification and Meity guidelines on Digital Signature for issuance & verification of Digital Signature.

8. Roles & responsibilities of Issuance of Digital Signatures:

a. Request for Digital Signature Certificates- Respective user shall submit the request for Digital Signature Certificates in duly filled application form with required documents to Digital Banking Department.
b. Issuance of Digital Signature Certificates- Digital Banking Department shall share application form and other documents with licensed CA and subsequently licensed CA will issue DSC to user.
c. Digital Signature Certificates owner shall ensure compliance of all the terms as a user as defined under Meity guidelines

9. Redressal of misuse/forgery of Digital Signature:

To avoid misuse or forgery of Digital Signature, following safety measures to be taken

a. Bank employees should securely store a private key using a certified cryptographic device.
b. Early detection of a fraud suspect is critical by implementing technical measures, best security practices and employee awareness.
c. Use multi-factor authentication, robust password policies, and secure key storage to minimize the risk of authentication vulnerabilities.
d. Always verify the authenticity and validity of digital certificates before accepting digitally signed documents. Make use of certificate revocation lists (CRLs) and trusted certificate authorities (CAs) to ensure the legitimacy of certificates.
e. Conduct regular audits of digital signature processes and security measures to identify potential vulnerabilities and areas for improvement.
f. Ensure that employees are trained to recognize and report phishing attempts.
g. Bank to ensure employees understand their roles and responsibilities for handling digital signatures.
h. Employees should handover the digital signature to Bank at the time of retirement/ exit from the Bank.

10. Standard Operating Procedure:

Bank shall issue comprehensive SOP for operations of Digital Signature and FAQs from time to time.

11. References

a. IT Act 2000 7 amendments therein

b. Guidelines for usage of digital signature in e-Governance (Dec -2010) by Ministry of Commerce & IT GOI.
c. Gazette Notifications from Meity dated 25/08/2015 for the digital signature (End entity) rules 2015.

Chapter IX

FASTag

1. Aim of this policy:

1.1. Introduction:

The FASTag Policy, hereinafter referred to as the "Tag Policy", is aimed at providing guidance to the employees and customers of Bank of Maharashtra (hereinafter called the "Bank"), and to manage the systems expected for governing the FASTag issuance.

The policy aims at the current business strategy of the Bank with regard to issuance of FASTag to its esteemed customers. The policy also lays out the various charges and terms associated with FASTag.

1.2. Governance and Intended Audience:

This policy is designed for the concerned departments/Branches within the Bank, who are dealing with products where FASTag issuance is required. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank and also of various regulators, including the NPCI/NETC.

The DBD Department shall be responsible for maintaining the supply to various zones.

2. Important Specifications of FASTag:

2.1 FASTag:

FASTag is an electronic toll collection system in India, operated by the National Highways Authority of India (NHAI).It employs Radio Frequency Identification (RFID) technology for making toll payments directly from the prepaid or savings account linked to it or directly toll owner. It is affixed on the windscreen of the vehicle and enables to drive through toll plazas without stopping for transactions.

2.2 Understanding a FASTag:

a. **Tag Serial Number**: It is a 16-digit number in which Frist 6 digits (607387) are the Bank ID/code, followed by the sequence 001 and last 7 digits are the serial numbers of our Bank Tags.

b. **Vehicle/Tag class**: The Vehicle class of any particular tag is mentioned on the Left top corner of each tag of our Bank.

c. **Customer care**: Each tag has the customer care number to contact for any support that needs to be extended.

d. **Color code**: The color of the tag varies with the vehicle class (VC) like Pink for VC12, Green for VC7, Yellow for VC6 etc.

e. **Logos**: Each Tag has the logo of the issuer/Bank, FASTag Trade mark, NHAI, NPCI, IHMCL trademarks.

f. **Bar code**: The customers FASTag serial number will be in the form of Bar code.

2.3 Types of FASTag and their Fees:

Bank issues various types of FASTags based on the type /category of the vehicle. These FASTags shall be allowed to use at any of the Tolls recognized by NETC/NHAI. Customers are required to submit requisite application form for type of FASTag they required, duly signed.

FASTags can be issued to both Bank and Non-Bank customers who has the vehicle. One wallet/One mobile number/One CIF can have multiple FASTags and there is no separate recharge for each Tag, recharge is done only for the wallet not for the Tag individually. Details of various FASTag variants along with the Fess details are as below:

Tag Class (Vehicle Class)	Class Description
4	Car / Jeep / Van / Tata Ace and similar mini light commercial vehicle
5	Light Commercial Vehicle
6	Three Axle Commercial Vehicle
7	Bus / Truck
12	4 to 6 axle
15	7 or more axle
16	Heavy Construction Machinery(HCM) / Earth Moving Equipment (EME)

3. Services Available on FASTag:

a. Retails & Corporate User Issuance
b. Automatic Wallet creation for customer
c. Top up and recharges of FASTag through different channels
d. Customization of mobile and web portals as per the requirement
e. Discount mechanism at local and product level
f. Customer account management and notifications
g. Inventory tracking
h. Date, time, toll plaza wise, customer wise, history view of previous FASTag issuances
i. Exception list management.
j. Integration with existing Bank's products- CBS/Debit Card/ M-banking/ E-wallet /Account – NETC system/ UPI
k. Availability of all the reports accessible, including customized reports
l. Dashboards with Customer Touch Point Activity and Payment History
m. Passage History, Rejection History and payment history of transactions.
n. Chargeback processing for Dispute Management
o. Tag Operations
p. Auto Top up facility through branch portal & customer portal
q. Desired Threshold limit and Amount to be recharged

r. Alert messages on wallet recharge
s. Update/Cancel the service any time

*Any addition /deletion/enhancement in services shall be done after approval of CDO/GM digital banking and shall be put up to ORMC on quarterly basis***.**

4. Usage Policy:

The FASTag shall be governed by the below terms and conditions:

a. The said Tag is valid only in India and only with respect to payments required to be made in INR. The Tag is permissible at all the recognized Tolls by NHAI/NETC with the country.

b. The FASTag user should ensure that the Tag is pasted on wind screen properly/visible for detecting at tolls.

c. FASTag is kept/handled at a safe place and under no circumstances whatsoever, should not allow the FASTag to be used by any other individual.

d. The Tag should be pasted immediately on the vehicle wind screen after assigning only.

e. The FASTag Account holder shall be responsible for all facilities granted by the Bank and for all related charges and shall act in good faith in relation to all dealings with the Tag and the Bank.

f. The Tag holder should notify the Bank immediately of any damage/loss/Theft of the tag at Mahaseva or by way of written communication to any of the branch of the Bank or such other mode as may be acceptable to the Bank.

g. The Tag Member shall be responsible for all facilities granted by BANK and for all related charges and shall act in good faith in relation to all dealings with the Tag and BANK. The Bank accepts no responsibility for any surcharge levied by any Concessionaire and debited to the balance available on the Tag, with the Transaction amount.

h. Any Transaction undertaken at a Participating Toll Plaza shall be conclusive proof that the charge recorded on such requisition was properly incurred for the amount and by the Tag Member using the Tag except where Tag has been lost, stolen or fraudulently misused, the burden of proof for which shall be on the Tag Member.

i. The Tag Member is responsible for all Transactions initiated by use of the Tag, except as otherwise set forth herein. Each time the Tag Member uses the Tag at a participating Toll Plaza, he authorizes BANK to reduce the funds available in the Tag Account by the amount of the Transaction.

j. The Tag Member agrees to pay BANK promptly for the negative balance. BANK also reserves the right to cancel/terminate the Tag should the Tag Member create one or more negative balances with the Tag.

k. Bank shall enable the NETC FASTag linked UPI QR code generator functionality on website/apps.

5. Customer Eligibility for FASTag Issuance:

FASTag can be issued to both existing/new Bank customers and even Non-Bank customers too.

5.1. **Bank Customers:**
Registration Certificate (RC) of the vehicle

5.2. **Non-Bank Customers:**
a. Photo identity proof
b. Valid Address proof as per RBI guidelines
c. Passport size photo of the vehicle owner
d. Registration Certificate (RC) of the vehicle

5.3. FASTag services should be available in Mobile Banking, Internet Banking and WhatsApp Banking to the maximum possible limit for better customer reach & usage.

5.4. At present Bank is issuing all types of Vehicle class Tags to its customers which are accessible at Nationwide all the toll plazas.

6. Other Form Factors:

Form Factor is the physical or virtual instrument that can be used in place of a card to undertake a payment/banking transaction.
FASTag cannot be issued in any other form factors other than the physical tags as per current available scenarios.

7. General Conditions:

a. If the customer's FASTag status is displayed as Low Balance/Hot listed etc. kindly load/recharge the customer's wallet to remove the flag (the **low Bal/Hot list** is due to negative Bal in the wallet)
b. If initially the vehicle number of the customer is not available to issue FASTag then the FASTag can be issued based on chassis number of the vehicle along with the copy of the vehicle purchased data (instead of RC initially). But later once the customer received the vehicle No., RC then the same should be updated in the portal in "**Update Vehicle Number**" option.
c. One wallet/One mobile number/One CIF can have multiple FASTags and there is no separate recharge for each Tag, recharge is done only for the wallet not for the Tag individually.
d. In case of raising request for refund of amount used/punched in CBS at the time of new FASTag registration, **reason should be mentioned/shared along with screen shots** [**E.g.:** Journal NO. is used after 2/3 days, Tag ID does not exist, Tag is not available in the inventory etc.] along with the evidences (screen shots) if any, Journal No., Amount, Account No., Date of T/n.
e. Branches before issuing the Tags to customer are instructed to check the Tag availability in their inventory as given below:

Branch Login-> Inventory -> Tag stock details

If the Tag is visible in the inventory, then only it should be issued. If not go ahead with other available Tag or raise an immediate request for tag mapping.

f. Bank shall ensure closure of all Multiple tags on same vehicle and ensure that only the latest issued tag as per the NETC mapper shall be active, except for previously issued tags in Hotlist or Blacklist exception code.

g. Bank shall issue the FASTag on VIN only from dealer location of the OEM (Original Equipment Manufacturer) of vehicles.
h. Bank shall update VRM for the tags issued within 90 days from the date of issuance.

8. Terms and conditions for issuance of Tags to customers:

a. BANK may issue the Tag to a customer on the request of the customer and pursuant to the customer making an Application for the Tag and agreeing to the applicable terms and conditions in the form and manner prescribed by BANK OF MAHARASHTRA in this regard.

b. BANK shall maintain records of these Applications and other Transactions in such manner as may be deemed suitable by BANK.

c. The Tag issued by BANK to the Tag Member shall be mandatorily affixed by the authorized representative of the Bank on the vehicle of the Tag Member with the license plate number specified by the Tag Member in the Application.

d. The Tag is not transferable and may only be used with respect to the vehicle on which the Tag has been affixed by the authorized representative of the Bank.

e. The tag holder shall be able to use the Tag only to the extent of the amount available on the Tag Account at any given point of time.

f. The Tag shall be activated subject to approval of the application by the Bank and a minimum amount being loaded on the Tag by the Tag Member. Such funds shall be loaded on the tag after deduction of the applicable charges/fees etc. payable by the Tag Member to BANK for availing the Tag.

g. The tag holder shall be bound to comply with these Terms and Conditions and all the policies stipulated by BANK from time to time in relation to the Tag. BANK may, at its sole discretion, refuse to accept the Application and to issue the Tag to the Tag Member.

9. Compliance with Other instructions

The issue of FASTag is subject to relevant instructions on wallet recharge, toll transaction, Auto top-up, security issues and risk mitigation measures, Bill desk/UPI fund transfers, Discount mechanism at local and product level, failed toll transactions, etc., issued by the NPCI/NETC/THMCL, Reserve Bank of India, Master Directions on Digital Payments Security Control, and Bank's guidelines for internal control system and mechanism, with regard to compliance of RBI guidelines, as amended from time to time.

10. Compliance

Compliance with Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation under the PMLA, 2002/NPCI/PPI guidelines:

The instructions/Directions on KYC/AML/CFT issued by RBI and Bank from time to time, shall be strictly adhered to in respect of all tags issued.

11. De-activating of FASTag:

Bank must deactivate a lost tag immediately on being informed by the customer and formalities or at the time of tag replacement the earlier tag will be automatically de activated.

12. Handling of Customer Complaints/ grievances:

Nature of Complaint	Handling Mechanism
Tag lost / stolen / damaged	Customer should contact Mahaseva /Branch through toll free number / email.
Amount debited from wallet extra/unwantedly	Customer should contact Mahaseva /Branch through toll free number / email.
Recharge/top-up failures	Complaints pertaining to Bank customers will be handled by Vendor and H.O, other bank customers to be handled with UPI vendor, H.O, DCRD team
Disputes regarding operations / service charges	Branch / Bank's Customer Care / Call Centre will handle such complaint.

13. Unsolicited commercial communication:

Bank may ensure that they engage telemarketers who comply with directions/ regulations issued by the Telecom Regulatory Authority of India (TRAI) from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)".

14. Security and Other Aspects:

a. The physical security & safe custody of the Tag is the sole responsibility of the customer. However, Bank shall ensure system security of the tags.

b. The liability of the customer/ bank is as per the Bank's Compensation policy which is reviewed as per the guidelines of Reserve Bank of India issued time to time.

15. Reconciliation & Settlement of transactions:

The first level of reconciliation of NETC-FASTag transactions will be done by M/s GI Technology Ltd (vendor) and reconciliation of BGL & CA accounts, refund, chargebacks will be handled by DCRD team.

16. Standard Operating Procedure:

Bank shall issue comprehensive SOP for KYC updation/renewal of FASTag, FASTag expiry, issuance of FASTag, settlement & reconciliation, Wallet limit, Redressal of Grievance, Escalation Matrix etc. and FAQs from time to time.

Chapter X

Digital Channel Reconciliation

1. Introduction:

Digital channel reconciliation is a policy or process that organizations implement to ensure accuracy and consistency between different digital channels or platforms. In today's interconnected world, businesses often utilize multiple digital channels, such as websites, mobile applications, social media platforms, and online marketplaces, to interact with customers, conduct transactions, and deliver services.

Digital channel reconciliation aims to address potential discrepancies and inconsistencies that may arise when data is shared or exchanged between these various channels. It involves comparing and aligning data from different sources to ensure that they match and reflect the same information accurately. By implementing a reconciliation policy, organizations can minimize errors, improve data integrity, enhance customer experience, and streamline their operations.

Implementing a digital channel reconciliation policy helps organizations maintain data integrity, improve operational efficiency, and provide a seamless and consistent experience to customers across different digital touchpoints. It also supports better decision-making by ensuring that accurate and reliable data is available to inform business strategies and initiatives.

The channels applicable under DCRD include ATM, POS & Ecommerce, UPI, IMPS, AEPS, Merchant Acquiring, Reconciliation and Cash management of ATMs & Recyclers.

a. Purpose:

The purpose of a digital channel reconciliation policy is to ensure accuracy, consistency, and reliability of data across various digital channels or platforms used by an organization. The policy serves several important purposes, including data accuracy, consistency, and reliability, which in turn enhances customer satisfaction, improves operational efficiency, supports decision-making, and mitigates risks for the organization.

The policy outlines responsibilities of various parties involved, the reconciliation process, corrective actions, reporting requirements and periodic audits to ensure compliance with various regulatory guidelines.

Reconciliation processes for digital channels handled by DCRD includes:

i. ATM
ii. POS (Point of Sale) & Ecommerce
iii. UPI (Unified Payment Interface)
iv. IMPS (Immediate Payment Service)
v. AEPS (Aadhaar Enabled Payment System)
vi. Merchant acquiring
vii. Reconciliation and Cash management of ATMs & Recyclers
viii. FASTag (GL Reconciliation)

The policy will be applicable to any new projects coming under DCRD before net review of this policy.

b. Objective:

The objective of a digital channel reconciliation policy are as below:

a. Operational Efficiency: Streamline the reconciliation of digital channels by reducing manual interventions, workarounds, and errors caused by inconsistent data. The policy aims to improve efficiency in data management, reconciliation processes, and GL operations.
b. Customer Experience: Enhance the customer experience by providing a seamless and cohesive support while resolution of Grievances. System will help to ensure that customers receive accurate and consistent information, leading to improved satisfaction and trust in the organization.
c. Risk Mitigation: Minimize risks associated with inaccurate or inconsistent information. The policy helps prevent financial losses, reputational damage, and customer dissatisfaction that can result from relying on erroneous data.
d. Monitoring and Auditing: Establish monitoring mechanisms and periodic audits to assess the effectiveness of the reconciliation process and identify areas for improvement. Regular monitoring helps identify and address discrepancies in a timely manner.
e. Continuous Improvement: Foster a culture of continuous improvement by incorporating feedback mechanisms, conducting regular reviews, and implementing enhancements to the reconciliation processes. The policy aims to adapt to changing business needs, emerging technologies, and industry best practices.

2. Stakeholder in Reconciliation & Responsibilities: -

The policy will be applicable for all the teams involved in the processes related to transaction life cycle. This includes

a. **DCRD** – The policy is primarily applicable to DCRD Team who is responsible for data collection from various sources, data upload to recon system, matching of transactions, post recon vouchers for unreconciled transactions, customer dispute handling for disputed transactions, clearing and settlement of interbank transactions.

At DCRD below teams are involved;

i. **DCRD Bank staff** – Bank staff allotted the project are responsible for end-to-end reconciliation of the particular project. This includes monitoring, getting the work done from responsible vendor team, release of vouchers provided by recon vendor.

ii. **Reconciliation Vendor** – The vendor personnel involved in the reconciliation processes are responsible for collection of data from various sources, data processing in recon system, matching of transactions, report generation, customer dispute handling.

iii. **POS Vendor** – The vendor handling end-to-end project of merchant acquiring (Debit/Credit card) business of the bank. In regards to reconciliation the team is responsible for clearing and settlement of POS transactions to the merchant in a timely manner, collection of MDR from merchants, customer dispute handling, reconciliation of the transactions with NPCI/VISA data.

b. CBS PMO – Transactions data from the CBS Team is the most important part of the reconciliation process. DCRD requires raw data from CBS to identify the accounting entries released during the transaction flow. This data is required to be matched with other data sources to reconcile the transactions. The team is responsible for sharing the raw transactions data of all the channels on a timely basis and ensure data accuracy.

c. ATM EFT Switch – EFT Switch team of the data center is responsible for carrying out the debit card transactions smoothly. In regards to reconciliation, the team is responsible for sharing the debit card raw transactions data on a timely basis and ensure data accuracy.

d. Financial Inclusion Team – Under Financial Inclusion scheme, bank is providing the transaction services to its customers through BC Points. Customers can carry out various transactions using Aadhar authentication at BC points such as cash withdrawal, deposit, fund transfer, balance inquiry etc. These transactions are routed through FI Switch and CBS. The FI team is responsible for sharing the AEPS raw transactions data on a timely basis and ensure data accuracy.

e. UPI Switch – UPI Switch is primarily responsible for smooth functioning of all UPI transactions in real time 24*7. In regards to reconciliation, team is responsible for sharing the UPI raw transactions data on a timely basis and ensure data accuracy.

3. Data Attributes:

Data attributes in digital channel reconciliation refer to the specific elements or characteristics of data that are considered during the reconciliation process. These attributes play a crucial role in ensuring accuracy, consistency of data across different digital channels. Here are common data attributes in digital channel reconciliation:

a. Transacting Channel
b. Transaction Real Time Reference Number (RRN)
c. Transaction Date and Time stamp
d. Transaction Amount
e. Transaction Account number [Beneficiary]

4. Frequency of Reconciliation/ Harmonization of TAT/Customer Compensation:

As per the guidelines issued by regulatory authority i.e. RBI Bank need to perform the reconciliation of all channels under this document purview daily [T+1] or Cycle wise as per availability of data files from stake holders. Reconciliation of system includes transaction reconciliation, Settlement of funding received from NPCI and settlement of transaction amount to customer account in case of related eventuality.

5. General Guidelines covering the TAT:

i) 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.

ii) 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, non-availability of cash in an ATM, 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.

iii) Terms like, Acquirer, Beneficiary, Issuer, Remitter, etc., have meanings as per common banking parlance.

iv) T is the day of transaction and refers to the calendar date.
v) 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.

vi) The term bank includes non-banks also and applies to them wherever they are authorized to operate.

vii) Domestic transactions i.e., those where both the originator and beneficiary are within India are covered under this framework.

6. **Harmonization of TAT and Customer Compensation:**

Reserve Bank of India vide circular DPSS.CO.PD No.629/02.01.014/2019-20 dated 20th Sep 2019 issued guidelines regarding "Harmonization of Turn Around Time (TAT) and customer compensation for failed transactions using authorized Payment Systems".

As per the circular, RBI issued guidelines regarding TAT to be followed by banks for reversal of failed transactions to the account of customers. In case of delay in crediting to customer, bank will have to pay an additional compensation of Rs100 per day from the TAT date. Bank shall follow TAT and compensation guidelines issued by regulator time-to-time.

7. Team Structure:

i. Digital Channel Reconciliation Department will be headed by executive (minimum Chief Manager). There are other officials in DCRD who performs the individual channel's daily reconciliation activity along with reporting and compliance.
ii. DCRD team is a blend of both specialist as well as Domain experts to take care of both technology and domain requirements.

8. Decision-Making Protocols:

As the Digital Channel's Reconciliation Department is under Digital Banking Department, all the Decision making protocols falls under the DBD policy will be applicable to digital Channel Reconciliation policy.

9. Incident Management and Root Cause Analysis:

Incident management and Incident categorization is to be done as per Information Technology Department's Incident Management Policy.

Escalation Matrix for Incident Reporting is as below:

Escalation Level	Designation
Level-1	Chief Manager DCRD
Level-2	Asst. General Manager DBD
Level-3	Chief Digital Officer

10. Monitoring and Auditing:

a. Monitoring:
Monitoring of Reconciliation process is done through reporting and Dash board.

b. Audit of DCRD and frequency of audit shall be guided by Inspection and Audit policy of the Bank. The audit of DCRD and Frequency of Audit may be approved and decided by ACE.

11. Documentation and Reporting:

DCRD in charge will be responsible for necessary documentations related to daily vouchers, GL tally reports, regulatory reports, Statutory reports, Internal External Audit Reports and periodic submission to higher authorities.

12. Vendor Personnel's at DCRD:

The Vendor team, seated at DCRD, is headed by the Vendor Project Team Lead (SPOC) who is responsible for the various activities being carried out by the vendor personnel seated at the DCRD.

13. Accountability

Vendor team is accountable for any SLA breach. The loss/damage, if any, that occurs to Bank / Customer, due to the code bug / system misbehavior / any attributable to Vendor team, shall attract penalty as per the SLA signed by the respective vendor.
The loss/damage, if any, that occurs to Bank / Customer, due to the intentional behavior of Bank Staff, shall attract accountability as per the OSR & Regulations of Bank.

14. Standard Operating Procedure:

Bank shall issue comprehensive SOP for settlement & reconciliation process of Digital channels, Escalation Matrix and FAQs from time to time.

15. Time limit for Data Preservation:

a. Raw files of NPCI/VISA/MasterCard and related transactions containing all vital information shall be preserved for a minimum period of 5 years immediately preceding the current calendar year.
b. Recon/Unrecon reports of NPCI/VISA/MasterCard and related transactions derived post processing the raw files shall be preserved for a period of minimum period of 10 years immediately preceding the current calendar year.

16. Reference

- RBI Harmonization of TAT Circular - DPSS.CO.PD No.629/02.01.014/2019-20

Chapter XI

Digital Banking Unit

1. Aim of this policy:

1.1. Introduction:

In-order to give boost to the digital economy and as our country marks 75 years of its independence, it was proposed in the Budget by Honorable Finance Minister Smt. Nirmala Sitharaman, to set up 75 Digital Banking Units (DBUs) in 75 districts of the country by the Scheduled Commercial Banks.

RBI has set up the guidelines for the establishment of Digital Banking Unit (DBU) which has been circulated through letter vide reference number RBI/2022-23/19 dated 07.04.2022.

DBU is specialized fixed point business unit / hub housing certain minimum digital infrastructure for delivering digital banking products & services as well as servicing existing financial products & services digitally, in both self-service and assisted mode, to enable customers to have cost effective/ convenient access and enhanced digital experience to/ of such products and services in an efficient, paperless, secured and connected environment with most services being available in self-service mode at any time, all year round.

1.2. Governance and Intended Audience:

This policy is designed for the concerned departments/Branches within the Bank, who are involved in the establishment of Digital Banking Unit. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank and also of various regulators, including the RBI/IBA.

The DBD Department shall be responsible for ensuring that the establishment of DBUs and services provided in DBU should be as per RBI/IBA guidelines.

Resource Planning Department shall do the identification and approval of DBU premise and assignment of various codes like MICR Code, Branch Code once DBU is established.

Corporate Service Department shall do the Civil work of DBU.

IT Department shall do the procurement as per business requirement.

Marketing Department shall do the Hoarding and Banner work for DBU.

2. Important Specifications of Digital Banking Unit (DBU):

2.1 Digital Banking Unit Model:

- A uniform model in all the Digital Banking Units with minimum services and minimum infrastructure made available.
- Each DBU shall be housed distinctly, with the separate entry and exit provisions. They will be separate from an existing Banking Outlet with formats and designs most appropriate for digital banking users.
- DBU to be categorized under “Banking Outlet” as defined under RBI.
- Separate Branch ID for DBU to help in generation of MIS on the usage of channels from the Unit.
- Paperless model as far as possible.

- Standardization:
  i. In terms of number of services and number of products offered across all DBUs.
  ii. However, Bank may offer any digitally feasible products / services on top of the minimum bouquet of products / services.

a) Classification of Digital Services offered to the customers under:
   i. Assets,
   ii. Liabilities,
   iii. Request Services.

b) Digital services / products to be offered to the customers under two different zones/areas
   i. Self Service Zone
   ii. Digital Assistance Zone

3. Bank's approach in setting up of Digital Banking Unit (DBU)

3.1 Digital Banking Unit (DBU) setup

The Bank, with the establishment of DBUs, envisions to provide its customer as well as non-customers with various digital banking services / products.

DBU will have "Uniform, Unified Digital User Experience under One roof" and will act as "Digital Experience Centre" for customers.

3.2 Products and Services:

a. Each DBU must offer certain minimum digital banking products and services. Such products should be on both liabilities and assets side of the balance sheet of the digital banking segment. Digitally value-added services to conventional products would also qualify as such. The DBUs are expected to migrate to more structured and custom made products, from standard offerings by use of its hybrid and high quality interactive capabilities.

b. The banks have the freedom to offer any other digital product or service in addition to the minimum bouquet to cater to the specific needs of the service area. Any product or service that can be provided digitally through internet banking or mobile banking can be provided in the DBU. Any product or service which a bank is not permitted to offer as per the provisions of Banking Regulation Act 1949, as amended from time to time, shall not be offered by the DBU.

Below is the list of bare minimum / add-on services / products that can be offered by Bank, at DBUs to customers / non-customers within two different zones/areas:

a. **Self Service Zone-** Cash withdrawal, Cash deposit, Online SB & Current Account opening, Internet Banking, Wealth management, Debit Card/Credit card hot listing, Grievance redressal system, FD/RD rates with calculator, Opening of FD/Rd account, Various loan rates with calculator, Bill Payments, Check book request, FASTag services, PMJDY account opening, Lead capturing for various loans, Passbook Printing, Cheque Deposit, Debit card issuance, Account Statement Generation and On boarding of customers for Government Schemes like Sukanya Samridhi, Senior Citizen saving schemes, PPF, PMJJBY, PMSBY, APY, end-to-end digital processing of loans, Kiosk with eKYC and video KYC

b. **Digital Assistance Zone-** 1) CIF data updation like e-mail id, address, etc, 2) Recovery / collection services, Credit Card issuance, 4) Cross selling of products like life/non–life Insurance, locker facility, etc., 5) Digital Kit for Merchants: UPI, QR code, BHIM Aadhaar, POS. 6) Mobile banking / internet banking/ UPI assistance. 7) Assistance for loan application and 8) Assistance and onboarding of Govt. sponsored schemes under National Portal.

3.3 Infrastructure and Resources

a. Each DBU shall be housed distinctly, with the separate entry and exit provisions. They will be separate from an existing Banking Outlet with formats and designs most appropriate for digital banking users.

b. For front-end or distribution layer of digital banking, each bank would choose suitable smart equipment, such as Interactive Teller Machines, Interactive Bankers, Service Terminals, Teller and Cash Recyclers, Interactive Digital Walls, Document uploading, self -service card issuance devices, Video KYC Apparatus, secured and connected environment for use of own device for digital banking, Video Call / Conferencing facilities, to set up an DBU. These facilities can be insourced or outsourced while complying with relevant regulatory guidelines.

c. The back-end including the Core Banking System and other back office related information systems for the digital banking products and services can be shared with that of the incumbent systems with logical separation. Alternatively, banks can adopt more core-independent digital-native technologies offering better scalability, flexibility in creating new / reusable digital environments through continuous development / software deployment and interconnectivity specifically for this business segment, based on their digital strategy.

d. If the digital banking segment of a bank uses an API layer (integration layer) to connect with external third-party application providers, the same should be tested in an isolated/ test environment before being integrated to bank's core systems backed by comprehensive risk evaluation and adequate documentation.

e. Bank can adopt an in-sourced or out-sourced model for operations of the digital banking segment including DBUs. The outsourced model should specifically comply with the relevant regulatory guidelines on outsourcing.

f. As the purpose of DBUs is to optimally blend digital infrastructure with 'human touch', remote or in situ assisted mode arrangements in right proportion should be planned and put in place by the banks.

g. The establishment of DBUs should be part of the digital banking strategy of the bank. The operational governance and administrative structure of the DBUs should be aligned with that of the Digital Banking Department of the bank. However, in order to accelerate digital banking initiatives, each DBU will be headed by a sufficiently senior and experienced executive of the bank, preferably Scale III or above for PSBs or equivalent grades for other banks who can be designated as the Chief Operating Officer (COO) of the DBU.

3.4 Branding and Logo of Digital Banking Units (DBUs)

As per the communication received from IBA dated 13/04/2022, it was informed that:

a. The DBUs are to be branded with uniform color pattern, Logo and design with theme on *Azadi Ka Amrit Mahotsav initiative*. IBA may engage agency for creation of Brand Name, Design, Color, Logo and Tagline.

b. The design to suggest demarcated spaces for self-service transactions and for customer engagement.

c. The Branding recommended is to be implemented by all the Anchor Banks.
d. The logo of Anchor Banks may also be displayed.

3.5 Metrics to measure performance of the DBUs

As defined by regulatory bodies IBA & RBI, different parameters to be considered to continuously monitor the performance of the DBUs, to meet the desired goals, are as under:

Sr.no	Monitoring Parameters
1	No. of new customer acquired.
2	No. of existing customers serviced for digital journey
3	No. of digital transactions initiated through DBU
4	CASA, Loans and other services through DBU
5	No. of leads generated and customers on-boarded for identified retails and Government sponsored schemes.
6	No. of end-to-end processing of loans.
7	New functionalities getting rolled out
8	Customer grievance redressal mechanism
9	Cost benefit analysis
10	Cyber security incidents in the DBU.

As per RBI guidelines dated 7th Apr 2022, below mentioned are the reporting requirements:

Sr.no	Reporting requirements
1	Banks shall report the Digital Banking Segment as a sub-segment within the existing “Retail Banking Segment” in the format of the Reserve Bank of India

	(Financial Statements – Presentation and Disclosures) Directions, 2021. It is clarified that the digital banking products / services applicable to segments other than 'Retail Banking' need not be reported at this stage
2	Performance update with respect to DBU shall be furnished in a pre-defined reporting format (being separately issued) to Department of Supervision, Reserve Bank of India on monthly basis by Digital Banking Department and in a consolidated form in Annual Report of the bank.
3	Resource Planning Department shall furnish information relating to opening, closure, merger or shifting of DBUs online through Central Information System for Banking Infrastructure (CISBI) portal to Department of Statistics and Information Management (DSIM), RBI as advised vide RBI circular DBR.No.BAPD.BC.50/22.01.001/2018-19 dated June 28, 2019 on 'Revision in Proforma and Reporting of Bank/ Banking Outlet (BO) details under CISBI.

3.6 Monitoring Process at Bank's end:

a. Report will be generated from Multi-Function Kiosks on the basis of DBU branch Code.
b. Monitoring of DBU will be made available through Dashboard.
c. Report to RBI will be submitted as per the pre-defined reporting format shared by RBI.

3.7 Monitoring of the functioning of DBUs

Steps for monitoring of the functioning of the DBUs to be followed by Bank, as defined by the regulators are as under:

a. DBU of the bank to be under the control of the Business Head/ Zonal Head of the geographical area in which DBU is established.
b. DBU to be monitored by the Digital Banking Department.
c. SOPs are being prepared for the services to be offered under DBU. The same will be completed & approved by competent authority before Going Live.
d. The Board of the Bank to be apprised on the performance of the DBU on quarterly basis.
e. Performance update of the DBU to be reported to RBI, in a pre-defined structure (to be received from RBI), on monthly basis in the first year of the establishment and subsequent segmental reporting in the Balance Sheet of the Bank.

Depending upon the performance report shared with RBI, the top performing DBUs may be rewarded and recognized.

4. Dress Code & Working Hours:

Dress Code:

In order to maintain the uniformity at all the DBUs, uniform dress code is proposed by the bank as below:

- **For Chief Operating Officer-** Officer should be in formal dress preferably with bank's tie/ badge.

- **Fixed Point BCs-** BCs appointed at DBU should be in formal dress.

Working Hours:

SN	Particulars	Timings
1	Self Service Zone	24*7*365
2	Digital Assistance Zone	10 AM to 5 PM on all working days

5. Machine/Hardware Deployment:

DBU shall have Multi-Function Kiosk, Account Opening Kiosk, ATM, Recycler, DMS, TAB, Laptop, Router & Switch, Printer and UPS & Battery.

6. Security Aspects

Bank to impart the following information to the end customers to ensure adequate cyber security awareness.

S.N	Particulars	Awareness Steps
1	Educating Customers visiting the DBU not to share sensitive details of their accounts & Cards, login credentials, PIN etc. to unknown persons.	Banners will be displayed inside DBU and messages will be sent through WhatsApp, SMS and Email etc.
2	Cyber Security awareness on phishing, hacking, spoofing, smishing, Denial of Service attack etc.	This may be spread through social media in vernacular language. Dos and Don'ts literature, posters will be displayed in Digital Banking Unit. Customer will be made aware for Do's and Don'ts when they visit the DBU.
3	Cyber Security Video	Cyber security Video will be displayed on DMS inside DBUs.
4	Random Quiz	Quiz on cyber security awareness will be published on social media channels
5	Guidance on customer grievance redressed procedures on digital frauds.	Banners and Posters will be displayed in DBU as well on DMS periodically.

7. Customer Grievances:

Bank shall provide adequate digital mechanism like Chatbot, AI Based Voice assistance etc. for real time assistance and redress customer grievances.

8. Role & Responsibilities

RBI in its circular vide reference number RBI/2022-23/19 dated 07.04.2022 defined the roles of Board of directors.

9. Standard Operating Procedure:

Bank shall issue comprehensive SOP for operations of DBU, functions of DBU, Roles & Responsibilities etc. and FAQs from time to time.

Chapter XII

Mobile Banking

1. Aim of this policy:

1.1. Introduction:

The Mobile Banking Policy, hereinafter referred to as the "Policy", is aimed at providing guidance to the employees and customers of Bank of Maharashtra (hereinafter called the "Bank"), and to lay down the systems and controls expected for Mobile Banking.

The policy documents govern the current business strategy of the Bank with regard to usage of Mobile Banking to its esteemed customers. The policy also lays out the various services and terms associated with Mobile Banking usage.

1.2. Governance and Intended Audience:

This policy is intended for the concerned departments within the Bank, who are dealing with products where Mobile Banking is a channels of service delivery. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank and also of various regulators, including the Reserve Bank of India.

The Digital Banking Department shall be responsible for maintaining the Mobile Banking service and shall work with the concerned departments to ensure that features proposed to the customers are implemented correctly within the various systems of the Bank.

The Digital Banking Department shall oversee the Mobile Banking availability and support to all the customers. IT Department shall do the procurement as per business requirement.

This policy shall be approved by the Board of Directors of the Bank and shall remain valid for a period of one year from such approval/ until reviewed/ policy enforce after one year (in case not reviewed).

2. Important Specifications of a Mobile Banking:

a. **Mobile Banking:**

i. Mobile Banking Application allows the customer to access his/her bank account using their Registered Mobile Number. Using the application customer can view account balance, mini statement, transfer funds and make utility bill payment. subject to prescribed terms and conditions.

ii. Mobile Banking is accessible to customers based on the CIF number and mobile number of the customer. Savings and Current account holders can available the Mobile Banking service

b. **MPIN / TPIN:**

PIN is a 4-digit secret number/ code which is generated by the customer at the time of registering for mobile banking for the purpose of security. MPIN is used to login into the mobile banking application and TPIN is used while making any financial transaction or service request.

Customers can also Reset/ change both the PIN through mobile banking after verifying their

identity.

3. Security Aspects

The Bank's Mobile Banking channels are protected by advanced security features, both physical and logical. Bank has considered various risks inherent in transacting over a public network such as the internet and has deployed appropriate security measures to protect customers. Required security is deployed to ensure safe and secure exchange of information between user Mobile Smart Phone and Banks Mobile application.

Technology used for mobile banking is secure and confirms to confidentiality, integrity, authenticity and non-repudiation.

Reserve Bank of India in its circular No. RBI/2010-11/494-DBS.CO.ITC.BC.No/6/31.02.008/ 2010- 11 has categorically defined the Roles and Responsibilities of end user for electronic banking transactions.

Bank will strive to disseminate awareness messages through available modes of communication as and when required basis, to keep its customers updated with secure environment.

Mobile Banking like any other technology driven service channels come with risks inherent to the internet ecosystem. However, prudent users have found ways to manage these risks. Banks worldwide have moved their customers to the Smart Phones & Computers, with enormous gains in efficiency and service quality. Bank has put in place secure and effective systems to mitigate risks from Bank's end. The customer must visualize the risks realistically and mitigate the same at their end. This includes proper handling of Username, passwords, Login and transaction PIN and overall safety of system at the user end.

Security Tips are provided on Maha Mobile Plus application (mentioning Do's & Don’ts for secure usage practices of mobile application along with a hyperlink, which leads to the website https://www.mahaconnect.in/ where Cyber Security Tips and awareness information regarding phishing email, internet Security, Browser Security, Wi-Fi security, Desktop Security and Password Security are provided in detail.

Bank shall implement proper level of encryption and security at all stages of the transaction processing in Mobile Banking. The endeavor shall be to ensure end-to-end encryption of the mobile banking transaction. Adequate safe guards would also be put in place to guard against the use of mobile banking in money laundering, frauds etc. The following guidelines with respect to network and system security shall be adhered to:

a) Implement application level encryption over network and transport layer encryption wherever possible.

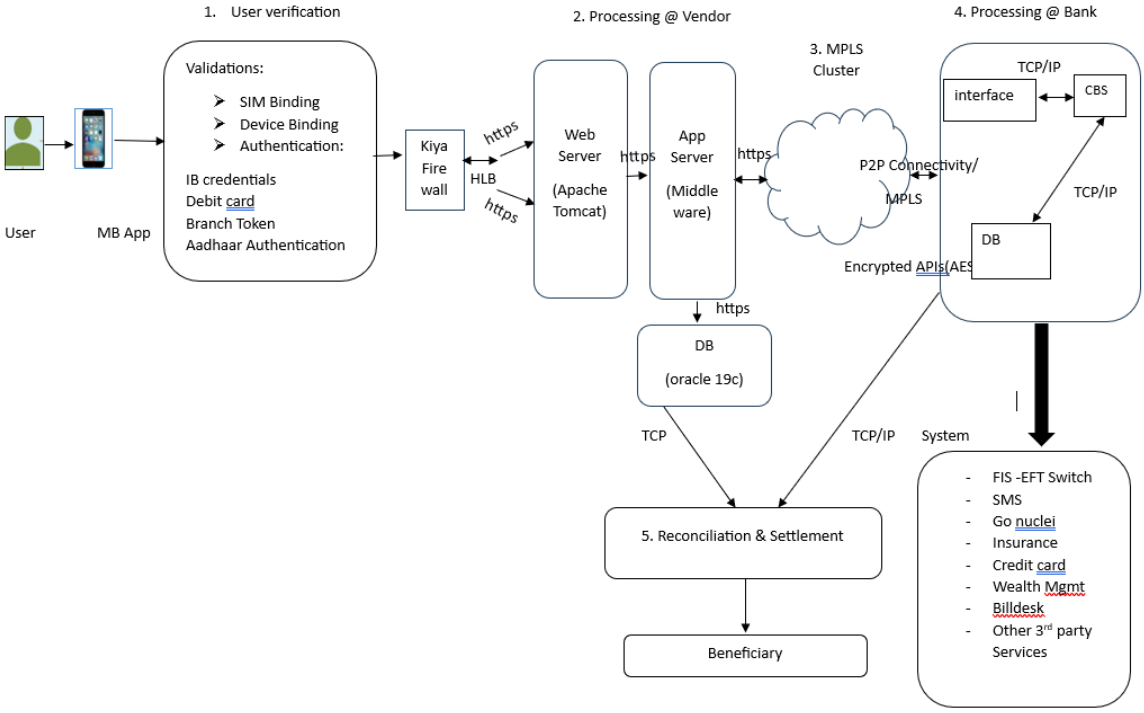
b) Establish proper firewalls, intruder detection systems (IDS), data file and system integrity checking, surveillance and incident response procedures and containment procedures.

c) Conduct periodic risk management analysis, security vulnerability assessment of the application and network etc at least once in a year.

d) Maintain proper and full documentation of security practices, guidelines, methods and procedures used in mobile banking and payment systems and keep them up to date based on the periodic risk management, analysis and vulnerability assessment carried out.

e) Implement appropriate physical security measures to protect the system gateways, network equipments, servers, host computers, and other hardware/software used from unauthorized access and tampering. The Data Centre of the Bank and Service Providers should have proper wired and wireless data network protection mechanisms

Digital Payment Cycle



4. Roles & Responsibilities:

Reserve Bank of India in its circular No. RBI/2010-11/494-DBS.CO.ITC.BC.No/6/31.02.008/ 2010- 11 has categorically defined the Roles and Responsibilities of end user for electronic banking transactions.

5. Mobile Banking - Application process & features

Maha Mobile Plus app is having both the functionality of mobile Banking and UPI. As per the industry norms, UPI shall be provided to both Bank and Non-Bank customers. However, providing services to non-bank customers for UPI shall be governed by Risk assessment done by Integrated Risk Management Department from time to time. Maha Mobile Plus app shall work on both data and Wi-Fi network; however, risk assessment shall be done by Integrated Risk Management Department from time to time. The Maha Mobile Plus app will adhere to the guidelines issued by RBI on mobile Banking/Internet Banking security controls dated 18.02.2021.

The following important features are available in Maha Mobile Plus:

a. Fund Transfer within Bank to self or to third party
b. Funds transfer to other Bank customers in India through IMPS/NEFT
c. Bill Payment through BBPS and tie up with Bill payment aggregators
d. View & download statement and M Passbook
e. Cardless cash withdrawal
f. Access Debit card / Credit card services
g. Reset login / transaction PIN
h. Loan EMI/ Deposit calculator
i. Pension Slip download
j. Pre-approved offers
k. Manage Payee
l. Apply for loans

m. Apply for Insurance

6. Mobile Banking – Transactions

All mobile banking transactions involving debit to the account shall be permitted only by validation through.

a. Two factor authentication (login pin & transaction pin- minimum 4-digit length)
b. One of the factors of authentication shall be MPlN or any higher standard.
c. Where MPlN is used, end to end encryption of the MPlN is desirable.
d. The MPlN shall be stored in a secure environment.
e. Additional authentication by way of OTP may also be explored.

Bank will set up suitable transaction limit in MB as decided time to time by limit review committee.

7. Mobile Banking -RBl Guidelines

The mobile Banking Policy will be governed by RBI guidelines from time to time. Some of the major circulars issued by RBI are as under:

- Reserve Bank of India (RBl) issued Master circular (DPSS.CO.PD.Mobile Banking. No.7107.73.001 /2014-15\ dated 01 .07.7014 and DPSS.CO.PD.Mobile Banking. No./2/02.23.001 /7016-2017 dated 01 .07.2016 containing rules / regulations / procedures prescribed to be followed by banks for operationalizing Mobile Banking in India.
- Reserve Bank of India vide Master direction RBI/2020-71/74 dated 18.02.2021 provides necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security contorts for digital payment products and services. Under Chapter IV of the Master Direction, RBI has issued instructions applicable to Regulated Entities offering/ intending to offer mobile banking/mobile payments facility to their customers through mobile application.

8. Grievance Redressal / Help Desk

Customer complaints / grievances arising out of mobile banking facility would be covered under the Reserve Bank - Integrated Ombudsman Scheme, 2021. Complaints raised by Maha Mobile user's fraudulent transactions shall be reported to Fraud Monitoring Cell/ Committee to look into the frauds arising out of usage of digital channels. Mobile Banking transactions would also be covered under the RBI's notification RBI/7017-18/15 BD.No.Leg.BC.78l09.07.005/2017-18 dated July 6, 2017 on Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions. Bank shall have proper Grievance Redressal mechanism and symmetrical escalation matrix as per Bank's Customer Service Policy. Bank shall have a help desk and disclose the details of the help desk and escalation procedure for lodging the complaints, on the websites.

9. Digital Payment Security Controls -Compliance of RBI Guidelines

RBI circular no. RBI 12070-21/74 DoS.CO.CS|TE.SEC.No.1852/3'1.01.015/2020-71 , dated 18.02.7021 on Master Direction on mobile Banking Security controls , provides necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security controls for digital payment products and services. As per the said circular, the provisions under this para shall be guided by the DPSC policy of the Bank. The contours of the policy, white discussing the parameters of any "new product"

including its alignments with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., should explicitly discuss about payment security requirements from Functionality, Security and Performance (FSP) angles such as:

a. Necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product/ services offered;
b. Availability of requisite infrastructure e.g. human resources, technology, etc. with necessary back up;
c. Assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency and rotted out after necessary testing for achieving desired FSP;
d. Capacity building and expansion with scalability (to meet the growth for efficient transaction processing);
e. Minimal customer service disruption with high availability of systems/ channels (to have minimal technical declines);
f. Efficient and effective dispute resolution mechanism and handling of customer grievance; and
g. Adequate and appropriate review mechanism followed by swift corrective action, in case any one of the above requirements is hampered or having high potential to get hampered.

The Board and Senior Management shall be responsible for implementation of this policy. The policy shall be reviewed periodically, at least on a yearly basis. CISO office has formulated the maiden policy on Digital Payment Security controls for the current year, as part of the overall product policy.

10. Customer Awareness

The Bank may advise from time to time for up gradation of user system/ software, such as Mobile Banking application /Browser etc., which are required for using mobile Banking services. There will be no obligation on the part of the Bank to support all the versions of user system/ software for accessing mobile Banking services of the Bank.

The Bank shall endeavor to provide Mobile Banking to user/ customer, such as ‘inquiry about the balance in his/her account(s), details about transactions, statement of account, request for issue of cheque-books, request for transfer of funds between accounts of the same user and other accounts and many other facilities as the Bank may decide to provide from time to time. The Bank at its sole discretion may also make additions /deletions to the mobile Banking Services being offered, without giving any prior notices or reasons. The Bank shall take reasonable care to, ensure the security of and prevent unauthorized access to the mobile Banking / UPI/ internet Banking Services using technology reasonably available. The user shall not use Mobile Banking services or any related service for any illegal or improper purposes.

Bank will endeavor to notify the user/customer through its website or through any legally recognized medium of communication found suitable by the Bank, regarding withdrawing/ suspending the Digital Payment Channel services wholly/ partially.

Bank will also endeavor to create awareness tips for using the mobile Banking applications, publish through Social Media, media. videos about products/ features/ and security Banking and host the same on the respective Radio, TV and any other forms of advertising.

11. Liability of the User and Bank

Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions shall be strictly as per the RBI and Bank's defined policies.

12. Third Party Links

The Site may provide hyperlinks to other applications/ websites not controlled by Bank of Maharashtra and such hyperlinks do not empty any endorsement, agreement on, or support of the content, products and /or services of such websites. Banks don't editorially control the content, products and /or services on such mobile applications/ websites and shall not be liable, in any nature whatsoever, for the access to, or the inability to access to, or the use, inability to use or content available on or through such mobile applications/websites.

Any party (third party), desirous of creating a link to the Bank's mobile application / website, is required to obtain prior written approval of the Bank before doing so. The Bank may, at its absolute discretion, give or refuse to give such approval for linking the Bank's website. The Bank may at its absolute discretion rescind any approval granted and require the removal of any [ink to the Bank's mobile application/websites at any time. Any link to the Bank's mobile application /website must be made directly to the homepage of our website and "framing" or "deep-linking" of our website or content is strictly prohibited. Any use or display of the Bank's - logos, trade names, trademarks, web content or material in any form is not permitted except with the prior written approval of the Bank's ORMC. Limited liability of customers in Unauthorized electronic Banking transaction shall be strictly guided by Customer services policy of the Bank.

13. General Conditions:

a. Bank customers should be on boarded as "Bank customer" only, using registered Mobile Number.
b. Mobile Banking service can be provided to existing customer having saving account and Current account under proprietorship.
c. Mobile Banking application should have SIM binding and device binding security control.
d. Registration of Mobile Banking can be completed using Debit Card, Aadhaar Card, Branch Token and Internet Banking any other modes as decided by bank time to time.
e. Bank shall have a provision to block a Mobile Banking application/ service immediately on being informed by the customer through Customer care or Branches/offices and formalities, if any, can follow within a reasonable period
f. Transaction through Mobile banking shall have at least Two-factor authentication (2FA) control.
g. Mobile Banking application cannot be installed if any remote access tool like team viewer, any desk etc. are installed on mobile.
h. Mobile Banking application can only be registered on mobile network data.
i. The user information, password etc will be encrypted and will have restricted access to proper storage under advise of CISO cell /regulatory guidelines.

j. DBD shall take up periodical review of registered users on MB database and take corrective action on deactivation/ deregistration of these users who have not utilized the app in last one year to avoid any misuse.

14. Standard Operating Procedure:

Bank shall issue comprehensive SOP for on-boarding of customer for Mobile Banking services, Registration of Mobile Banking, De-registration of Mobile Banking services, Change of Login and Transaction PIN, services on Mobile Banking, features of Mobile Banking, Transaction limit of Mobile Banking, Escalation matrix etc. and FAQs from time to time.

15. Reference:

a. Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks dated 01.07.2026 (Updated as on November 12, 2021)

Chapter XIII

Internet Banking

1. Aim of this policy:

1.1. Introduction:

The Internet Banking Policy, hereinafter referred to as the "Policy", is aimed at providing guidance to the employees and customers of Bank of Maharashtra (hereinafter called the "Bank"), and to lay down the systems and controls expected for managing the Internet Banking usage.

The policy documents govern the current business strategy of the Bank with regard to usage of Internet Banking by its esteemed customers. The policy also lays out the various terms associated with Internet Banking usage.

1.2. Governance and Intended Audience:

This policy is intended for the concerned departments within the Bank, who are dealing with products where Internet Banking is available. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank and also of various regulators, including the Reserve Bank of India.

The Digital Banking Department shall oversee the availability of Internet Banking to various customers. IT Department shall do the procurement as per business requirement.

This policy shall be approved by the Board of Directors of the Bank and shall remain valid for a period of one year from such approval/ until reviewed/ policy enforce after one year (in case not reviewed).

2. Important Specifications of Internet Banking:

Internet Banking:

i. Internet banking, also known as online banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website.
ii. Online banking allows customer to conduct financial transactions via the Internet.
iii. Online banking offers customers almost every service traditionally available through a local branch including deposits, transfers, and online bill payments.
iv. Internet Banking in India - Guidelines dated 14 Jun 2001, Internet Banking in India – Guidelines dated 20 Jul 2005, Internet Banking – Internet based platforms for dealing in Foreign Exchange dated 22 Aug 2006. The recommendations of the 'Working Group on Internet Banking' referred to in the RBI circular on Internet Banking in India - Guidelines dated June 14, 2001, Internet Banking - Internet Based Platforms for Dealing in Rupee Vostro Accounts dated 15 Nov 2007 7. Customer Protection for Unauthorized Electronic Banking Transactions policy refers to RBI Circular reference: DBR.No. Leg.BC.78/09.07.005/2017-18 dated July 6, 2017. Master Directions on Digital Payment Security Controls dated February 18, 2021. RBI Advisory Digest – Consolidation of controls prescribed in the advisories issued dated March 27, 2024.

Password policy:

Login password/ Transaction password:

i. Must be between 8-20 characters in length
ii. At least one number, special character, uppercase letter and lowercase letter
iii. No spaces in between
iv. Passwords are case sensitive
v. Transaction password cannot contain the associated login ID/username/password
vi. Change password often.
vii. The same password should not be used across multiple accounts or platforms.
viii. Do not include any personal information in your password (e.g. address, phone number, birthdate).
ix. Do not write it down or share it with anyone else.
x. The login password/transaction password shall be subject to changes from time to time as per password policy in IT policy

Types of financial transactions through Internet Banking:

National Electronic Fund Transfer (NEFT)

i. National Electronic Funds Transfer (NEFT) is a nation-wide payment system facilitating one-to-one funds transfer. Under this, individuals, firms and corporates can electronically transfer funds from any bank branch to any individual, firm or corporate having an account with any other bank branch and vice versa in the country.
ii. The fund remittances will be restricted to a maximum of Rs. 50,000/- per transaction.
iii. The limit of fund remittance may be enhanced upon receipt of request from customer.
iv. RTGS is defined as the continuous (real-time) settlement of funds transfers individually on an order by order basis (without netting). 'Real Time' means the processing of instructions at the time they are received rather than at some later time; 'Gross Settlement' means the settlement of funds transfer instructions occurs individually (on an instruction by instruction basis).
v. The RTGS system is primarily meant for large value transactions. The minimum amount to be remitted through RTGS is 2 lakhs. There is no upper limit for RTGS transactions.

Electronic Clearing System (ECS)

ECS is an alternative method for effecting payment transactions in respect of the utility-bill-payments such as telephone bills, electricity bills, insurance premium, card payments and loan repayments, etc.,

Immediate Payment Service (IMPS)

IMPS offers an instant, 24X7, interbank electronic fund transfer service through mobile phones. IMPS is a tool to transfer money instantly within banks across India through mobile, internet and ATM.

Foreign Remittances

Customers can initiate foreign exchange transaction using Internet Banking. The transactions upto USD 10,000/- or equivalent shall be processed on Daily Card Rate

published by bank. While processing the transaction, Bank shall ensure the FEMA guidelines issued from time to time.

Mahasecure (2FA – Second Factor Authentication)

"MAHASECURE", second- factor authentication facility for internet Banking customers has been made available as an optional facility to provide customers with best & secured services.

Important Features of Mahasecure:

a) Available on all devices - desktops, laptops, tablets & smart phones.

b) Supported on all operating systems - Windows, Mac OS, iOS, Android.

c) Quick banking activities like check account balance, fund transfer, pay bills are just a click away.

d) Military grade security through a secure private network (REL-ID Network) protecting against loss of funds.

e) Max 20 devices can be enrolled under Mahasecure using the secured question and answer already set and Mahasecure login password.

As soon as the Internet Banking user loges in into IB (Mahaconnect), post the activation, the activation key and verification keys are sent to the user through SMS on registered mobile number. The user is expected to install the Mahasecure app and register using the keys shared. In the process user has to set the secured question and answer and set the Mahasecure login password.

3. Customer Eligibility for Availing Internet Banking:

4.1. **Retail Customers**:

a) Retail customers can activate internet Banking by registering themselves, using "**New User Register**" link. In some exceptional cases, Retail users can also submit physical application form through branch for creation of user lDs.
b) The User should submit necessary documents and information as required by the Bank.

4.2. **Corporate Customers:**

a. Data of all new requests of Corporate users will be routed Branch shall obtain application and signed documents as specified, signed by all authorized signatories and verify that the application is signed by the authorized signatories. After verifying the correctness of signatures with account opening form, the application data for creation of users will be inserted by maker user at branch and verified by checker user at branch.
b. In case of addition of users/ modification of rights of users etc., in Corporate application, the same will be forwarded to Digital Banking department after verification / attestation of customer signature by Branch.
c. The basis of activating internet Banking services is customer lD. On specific request, the user/ customer can restrict access to any particular account in internet Banking.

4. Redressal of grievances

Turn Around Time (TAT) and customer compensation for fraudulent transactions shall be governed by Bank's Customer Compensation Policy

a. The TAT for resolution of grievances related to internet Banking transactions shall be as per Grievance Redressal Policy and subsequent revisions from time to time. This is in compliance with guidelines of RBI circular on Digital Payments Security Controls to have efficient and effective dispute resolution mechanism and handing of customer grievances
b. Customer complaints / grievances arising out of Internet Banking facility would be covered under the Banking Ombudsman Scheme. Complaints raised by internet Banking users for fraudulent transactions shall be reported to Fraud Monitoring Cell to take into the frauds arising out of usage of digital channels.

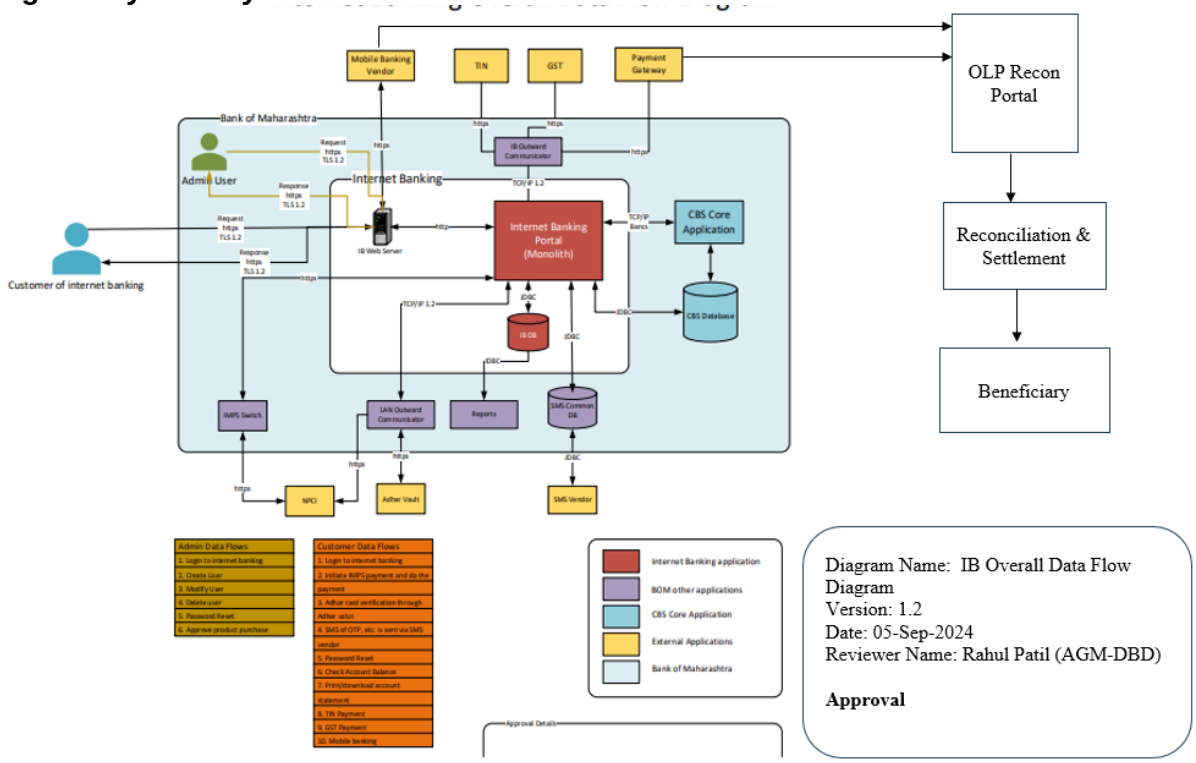
5. Security and Other Aspects:

i. The Bank's internet Banking channels are protected by advanced security features, both physical and logical.
ii. Bank has considered various risks inherent in transacting over a public network such as the internet and has deployed appropriate security measures to protect customer's information.
iii. Required security is deployed to ensure safe and secure exchange of information between user and Bank & other parties.
iv. Technology used for internet Banking is secure and confirms to confidentiality, integrity, authenticity
v. The responsibilities of Bank include maintaining confidentiality of log-in password(s), ensuring security of information etc.
vi. Adhering to security policies, procedures, standards, and guidelines Bank will strive to disseminate awareness messages through available modes of communication as and when required basis, to keep its customers updated with secure environment.
vii. Cyber Security Tips and awareness information regarding Phishing email, internet Security, Browser Security, Wi-Fi security, Desktop Security and Password Security are provided in detail. A hyperlink is provided on login page of internet Banking application where users have to accept the terms and conditions and disclaimer of Bank's internet Banking services. It is mandate that the users have to read and agree the internet Banking services provided by the Bank as per the terms and conditions mentioned.
viii. Security by design aspect shall be implemented by referening digital payment security controls.

6. Standard Operating Procedure:

Bank shall issue comprehensive SOP for on-boarding of customer for Internet Banking services, De-registration of Internet Banking services, Change of Login and Transaction PIN, services on Internet Banking, Usage policy, Escalation Matrix, features of Internet Banking etc. and FAQs from time to time.

Digital Payment Cycle



7. General Conditions:

a) Bank customers should be on boarded as “Bank customer” only, using registered Mobile Number.

b) Mobile Banking service can be provided to existing customer having saving account and Current account under proprietorship.

c) Bank shall have a provision to block Internet Banking application/ service immediately on being informed by the customer through Customer care or Branches/offices and formalities, if any, can follow within a reasonable period

d) Transaction through Internet Banking shall have at least Two-factor authentication (2FA) control.

e) Bank shall issue detailed operational guidelines regarding for usage of Internet Banking Application

f) The user information, password etc will be encrypted and will have restricted access to proper storage under advise of CISO cell /regulatory guidelines.

g) DBD shall take up periodical review of registered users on IB database and take corrective action on deactivation/ deregistration these users who have not utilized the app in last one year to avoid any misuse.

Chapter XIV

CREDIT CARD POLICY

1. Introduction

The term "**Credit Card**" usually/generally refers to a plastic card assigned to a cardholder, usually with a credit limit, that can be used to purchase goods and services on credit or obtain cash advances without having balance in the account. The Credit Card is a Credit product in which a sanctioned limit is given to customer within which customer can do the transactions without any restrictions. Bill of credit card will be generated on monthly basis on a predefined date as approved by Bank.

Credit cards allow cardholders to pay for purchases made over a period of time, and to carry a balance from one billing cycle to the next. Credit card purchases normally become payable after an Interest Free Credit period, during which no interest or finance charge is imposed. Interest is charged on the unpaid balance after the payment is due. Cardholders may pay the entire amount due and save on the interest that would otherwise be charged. Alternatively, they have the option of paying any amount, as long as it is higher than the minimum amount due, and carrying forward the balance. Credit card can also be used for carrying out International transactions.

The credit card scheme involves following parties viz.

a) **Card holder:** Person who is authorized to use the card.
b) **Card Issuer:** Banks/ NBFCs/Financial Institutions which issue credit cards.
c) **Merchants Entities:** Who agree to accept credit cards for payment of Goods & Services.
d) **Merchant acquires:** Banks/NBFCs/ Financial Institutions which enter into agreements with merchants to process their credit card transactions
e) **Credit Card Association.:** Group of Card issuing Banks or Organizations that set common transaction terms for merchants, issuers and acquirer. Some major associations are Visa, MasterCard, Rupay, American Express and Discover issues license card issuers to issue credit cards under their trade mark e.g. Visa, Rupay and Master Card and provide settlement services for their members (i.e. Card Issuers and Merchant Acquirers).

The Credit Card Cell of the Bank shall be responsible for implementing the credit card scheme in the Bank.

2. Purpose

To provide a basic framework based on rules/regulations/standards/practices as prescribed by RBI and other regulators for carrying out of credit card business and to ensure best customer practices. It is necessary to adopt adequate safeguards and implement the guidelines in this policy in order to ensure that the card operations are run on sound, prudent and customer friendly manner.

3. Scope

This policy is applicable to all the staff members of Bank, subsidiaries and any third party engaged by the Bank.

3.1. Issue of Credit Cards

Bank will undertake Credit Card business independently. At present, prior approval of RBI is not necessary if Credit card is issued either independently or in tie-up arrangement with other card issuing Banks. If Bank decides to issue credit cards through its subsidiary in future, then prior approval of Reserve Bank of India will be obtained by the Credit Card Cell.
Bank will ensure prudence while issuing Credit Cards and independently assess the credit risk while issuing cards to persons especially to students and others with no independent financial means.
Necessary approval of board along with approval of New Product Committee for launching specific credit card will be taken by the Credit Card Cell.

a) Customer Acquisition:

i. Bank should provide a one-page Key Fact Statement along with the credit card application containing the important aspects of the card such as rate of interest, quantum of charges, among others. In case of rejection of a credit card application, bank will convey in writing the specific reason/s which led to the rejection of the application.

ii. The MITC shall be published/sent separately to the customers, at the acceptance stage (welcome kit) and in important subsequent communications. The MITC shall be provided to the customer at the time of on boarding and each time, a condition is modified with notice to the customer. The MITC and copy of the agreement signed between the Bank and cardholder shall be sent to the registered email address of the cardholder or postal address as per the choice of the customer.

iii. Bank may consider introducing, at the option of the customers, an insurance cover to take care of the liabilities arising out of lost cards, card frauds, etc. In cases where the Bank is offering any insurance cover to their cardholders, in tie-up with insurance companies, the Bank shall obtain explicit consent in writing or in digital mode from the cardholders along with the details of nominee/s.

iv. The issue of unsolicited cards/upgradation is strictly prohibited. In case, an unsolicited card is issued/existing card upgraded and activated without the explicit consent of the recipient and the latter is billed for the same, the Bank shall not only reverse the charges forthwith, but also pay a penalty without demur to the recipient amounting to twice the value of the charges reversed. In addition, the person in whose name the card is issued can also approach the RBI Ombudsman who would determine the amount of compensation payable by the Bank to the recipient of the unsolicited card as per the provisions of the Ombudsman Scheme, i.e., for loss of complainant’s time, expenses incurred, harassment and mental anguish suffered by him/her.

v. There have been instances where unsolicited/applied-for cards have been misused before reaching the persons in whose names these have been issued. It is emphasised that any loss arising out of misuse of such unsolicited cards shall be the responsibility of the Bank only and the person in whose name the card has been issued shall not be held responsible for the same.

vi. Bank shall seek One Time Password (OTP) based consent from the cardholder for activating a credit card, if the same has not been activated by the customer for more than 30 days from the date of issuance. If no consent is received for activating the card, Bank shall close the credit card account without any cost to the customer within seven working days from date of

seeking confirmation from the customer. In case of a renewed or replaced card, the closure of an inactivated card shall be subject to payment of all dues by the cardholder.

vii. Bank shall not report any credit information relating to a new credit card account to Credit Information Companies prior to activation of the card. Any credit information relating to such inactivated credit cards already reported to Credit Information Companies shall be withdrawn immediately.

viii. The written consent of the applicant shall be required before issuing a credit card. Alternatively, Bank may use other digital modes with multifactor authentication to obtain explicit customer consent. Such alternative digital modes, if any used by the Bank, shall be communicated to the Department of Regulation, Reserve Bank of India.

ix. Bank should ensure that the telemarketers engaged should comply with directions/regulations on the subject issued by the Telecom Regulatory Authority of India (TRAI) from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)". The Bank's representatives shall contact the customers only between 10:00 hrs and 19:00 hrs.

x. The decision-making power for issue of credit card to a customer shall remain only with the Bank and the role of the Direct Sales Agent (DSA)/Direct Marketing Agent (DMA)/other agents shall remain limited to soliciting/servicing the customer/ account.

b) Underwriting standards:

i. Bank shall ensure prudence while issuing credit cards and independently assess the credit risk while issuing cards to persons, taking into account independent financial means of applicants.

ii. As holding several credit cards enhances the total credit available to any consumer, Bank shall assess the credit limit for a credit card customer taking into consideration all the limits enjoyed by the cardholder from other entities on the basis of self-declaration or credit information obtained from a Credit Information Company.

iii. Bank shall ensure complete transparency in the conversion of credit card transactions to Equated Monthly Instalments (EMIs) by clearly indicating the principal, interest and upfront discount provided by the merchant/Bank (to make it no cost), prior to the conversion. The same shall also be separately indicated in the credit card bill/statement. EMI conversion with interest component shall not be camouflaged as zero-interest/no-cost EMI.

iv. Bank shall ensure that loans offered through credit cards are in compliance with the instructions as per loan policy of bank as amended from time to time.

v. Bank shall ensure that the credit limit as sanctioned and advised to the cardholder is not breached at any point in time without seeking explicit consent from the cardholder.

3.2. **Types of credit cards**

With prior approval of Board, Bank may issue following types of credit cards as under:

a) **Primary Credit Card:** The Cards issued to a customer after assessing the credit risk of the customer. These Credit Cards are called Primary Credit Cards and the Card holder is called Primary Card Holder.

b) **Add-on Credit Cards**: Add on cards are subsidiary to the primary card, may be issued with the clear understanding that the liability will be that of the primary cardholder. Credit limit for add-on card may be same as the primary card or sub-limit of primary card. All the add-on cards will be linked to one primary card.

c) **Corporate Credit Card**: While issuing corporate credit cards, the responsibilities and liabilities of the corporate and its employees should be clearly specified. The liability of the corporate/business entity on account of business cards shall form part of their total assessed credits for compliance to instructions issued by the Bank on Exposure Norms as well as Prudential norms on Income Recognition, Asset Classification and Provisioning pertaining to Advances.

d) **Co-branded Credit Card:** Bank will issue Co-Branded Credit Cards with other Banking or non-Bank entities. However, role of the Banking or non-Bank entity under the tie-up arrangement should be limited to marketing/ distribution of the cards or providing access to the cardholder for the goods/services that are offered. While issuing Co-Branded Credit Cards, Bank will undertake due diligence of the Banking or non-Bank entity to protect itself from any reputational risk.

e) **Business Credit Card:** Bank may issue business credit cards to business entities/individuals for business expenses. The business credit cards may also be issued as charge cards, corporate credit cards or by linking a credit facility such as overdraft/cash credit provided for business purpose as per the terms and conditions stipulated for the facility concerned. Bank will put in place an effective mechanism to monitor end use of funds. Business credit cards can be issued together with add-on cards wherever required.

f) **Virtual Credit Card (VCC):** A Virtual Card creates an extra layer of security for making a credit card payment. A Virtual card is a randomly generated 16 digit number associated with actual credit card account. The Virtual Credit Card is offered as a way to protect against the fraud at “card not present” transactions. Once a purchase with virtual credit card is done the number is retired and never used again. This prevents fraudster from stealing actual credit card number.
Virtual Cards will be governed by the existing guideline for Physical Credit Cards.

g) **General Credit Card (GCC):** GCC shall be issued in the form of a credit card and the terms and conditions of the credit facilities extended in the form of GCC shall be as per the Board approved policies of the bank, within the overall framework laid down by Reserve Bank.

The due diligence of Banking or non-Bank entity will generally include KYC, management and financial due diligence besides taking into account necessary permissions, reputation of the entity in the market, pendency of any tax related or legal case against the company, information on customer handling, management resolution for entering into tie up business etc. The customers of non-Bank entities must open regular saving Bank account with Bank before making application for credit card.
The NBFC entering into tie-up should ensure confidentiality of the customer’s accounts. The co-branding NBFC should not reveal any information relating to customers obtained at the time of opening the account and should not be permitted to access any details of customer accounts that may violate Bank’s secrecy obligations.
These entities must comply with the points mentioned under Customer Confidentiality and Privacy section.

Role of the co-branding partner will be decided at the time of agreement with bank. It can be referral only / they may undertake part / full risk accordingly the role and responsibility of co-branded partner will be decided.
Customer complaints arising out of deficiency in the credit card service by co-branding partner shall be the responsibility of the bank. The credit card grievances will be handled by bank as per banks existing customer grievance policy.

3.3 Closure of Credit Card

a) Any request for closure of a credit card shall be honoured within seven working days by the Bank, subject to payment of all dues by the cardholder. Subsequent to the closure of credit card, the cardholder shall be immediately notified about the closure through email, SMS, etc. Cardholders shall be provided option to submit request for closure of credit card account through multiple channels such as helpline, dedicated e-mail-id, Interactive Voice Response (IVR), prominently visible link on the website, internet banking, mobile-app or any other mode. Bank shall not insist on sending a closure request through post or any other means which may result in the delay of receipt of the request. Failure on the part of the Bank to complete the process of closure within seven working days shall result in a penalty of ₹500 per calendar day of delay payable to the customer, till the closure of the account provided there is no outstanding in the account.

b) If a credit card has not been used for a period of more than one year, the process to close the card shall be initiated after intimating the cardholder. If no reply is received from the cardholder within a period of 30 days, the card account shall be closed by the Bank, subject to payment of all dues by the cardholder. The information regarding the closure of card account shall also accordingly be updated with the Credit Information Company/ies within a period of 30 days.

c) Subsequent to closure of credit card account, any credit balance available in credit card accounts shall be transferred to the cardholder's bank account. Bank shall obtain the details of the cardholder's bank account, if the same is not available with them.

3.4 Basic Feature of BoM Credit Card

i. Bank can issue Card in tie up with VISA, MasterCard and RuPay Associations.
ii. Bank can give Reward points on activation of credit card, transactions made on card, as decided by Bank from time to time after taking necessary approval from competent authority.
iii. Bank can extend Flexi Pay / EMI facility on certain transactions as per criteria decided by Bank.
iv. Bank can extend Balance Transfer Facility from other Bank Credit Card under Equated Monthly Instalment (EMI) scheme with repayment period of 6 months.
v. Bank can tie-up with third party to run loyalty programme for increasing transaction.
vi. Bank can make tie up arrangement with various merchants for offering EMI at source and other discount card offers.
vii. Bank will be providing various options to customers for paying credit card dues e.g. auto debit facility, payment through other bank debit cards / internet banking, UPI, account & IFSC code etc.
viii. Bank may issue Virtual Credit cards with in the frame work defined by RBI.

3.5 Limit for Credit Card

a. **For existing account Holders:**

Limit to be decided based on the score obtained as per Scoring Model for assessment of credit risk of applicants. There will be two separate scoring model for different class of customers i.e Salaried & Businessman / self-employed.

b. For non-customers:

Non-customers is also referred as “New To Bank” customers i.e. the customers who do not have Banking relation with us. As of now bank is not issuing credit cards for non-customers. However, in future bank may issue credit cards to non-customers also after prior approval from CRMC . In this category as bank is not having any existing customer relationship. So bank has to identify these customers, complete the due diligence including KYC, risk assessment etc. This will be additional activity over and above the same given in above point. The detail SOP will be issued prior to launch of credit card for non-customers.

Based on risk assessment of customer, the credit limit will be decided based on score obtained as per Scoring Model defined by Bank. There will be two separate scoring model for different class of customers i.e. Salaried & Businessman/self-employed. However, maximum credit limit as per scoring model shall be sanctioned as per the above mentioned of delegated powers of lending.

c. For bank’s existing valuable loan customers

Bank will be offering credit card to its existing valuable loan account customers, who are already availed loan facility with bank and is having good track record of payment. The credit risk has already been accessed by the bank and required documents are already collected. Bank will be issuing credit card to such customers without collecting documents again only by getting consent in writing or digitally. This will help bank in cross selling more products and enhancing the banking relationship without increasing much credit risk. The credit card limit to be sanctioned to the customers shall be based on the Scoring Model and additional weightage for existing valuable loan customers. The sanctioning authority for the credit card limit shall be as per the circular of delegated powers of lending.

d. Corporate clients:

Bank may issue BoM Credit Cards to their corporate clients as part of working limit sanctioned to them as part of MPBF. In this case, bank will sanction over credit card limit to the corporate client. The corporate client will be providing the list of authorised signatories to whom the corporate credit card needs to be given along with credit card limit as required by them. The overall capping of corporate limit will be defined as per sanction to the corporate. It means as part of policy there is no upper limit.

e. **Secured Credit Cards:**

Students and other persons with no independent financial means and eligible to enter into contract will be issued Credit Card on secured basis i.e. against deposit with Bank. Maximum limit for secured Credit Card will be 80% of the deposit. Lien shall be created on the security for such credit cards by credit card cell, HO. FDR to be preserved & stored at branch along with the application and KYC details. The Fixed deposit receipt to be duly discharged and declaration to break the FDR on default to be taken as per existing LAD document guidelines. In case of default by the credit card holder, Bank has the right to liquidate the security to recover the dues when the outstanding balance of card is more than 90% of security value or in case of default whichever is earlier. Credit card holder should be made aware of this and acknowledgment of the same should be obtained. The detailed information about the card is added in Annexure III.

Limit for Ex-employee of Bank will be defined as per the scoring model for normal customers.

Deviation in the credit card policy for any customer because of eligibility criteria can be approved from Deputy General Manager / General Manager handling the department.

3.6 Timeline for Issuance of Credit Card:

The total turnaround time involved in issuance of Credit Card till physical delivery is 2 weeks subject to completion of all documents and adherence of Bank's guidelines.

3.7 Upgradation / Limit Enhancement of Credit Cards:

Process for enhancement of Credit Limit shall be decided by the CRMC.

3.8 Tokenization of Credit Cards:

Tokenization refers to replacement of actual card details with an alternate code called the "token", which shall be unique for a combination of card, token requestor (i.e. the entity which accepts request from the customer for tokenization of a card and passes it on to the card network to issue a corresponding token) and device.

4. Insurance Coverage (Life, Accident or Health)

In cases where Bank decides to offer insurance coverage to the Credit Card customers, in tie-up with insurance companies, branches will obtain in writing details of nominees or self-declaratory letter in case customer does not wish to nominate anyone and send the same to Credit Card Cell. Credit Card Cell will ensure that nomination details are recorded by the insurance company. Branches will issue letter to the credit card holder indicating the details regarding the name, address and telephone number of the Insurance Company which will handle the claim along with nomination details.

Bank may offer insurance of card transactions to indemnify loss occurred to the customer due to fraud, hacking, cloning of card etc. Maximum insured amount shall be limit allowed on card. Premium of the insurance shall be charged to the card after getting written confirmation from respective card holder.

5. Eligibility Criteria for Credit Card:

The eligibility for credit card can be decided based on following parameters as under:

i) Income Criteria (Salaried / Self Employed / Businessman etc.)

ii) Age Criteria as decided by Bank from time to time. Minimum entry age is 18 years and maximum entry age is 65 for all types of card except in case of Secured Credit Card where there is no restriction on maximum entry age.

iii) Minimum CIBIL score of individual for credit card eligibility should be 750. For customers having no credit history/new to credit having CIBIL score 1 or -1 are also eligible.

iv) Credit Card can be issued Resident Indian and NRIs.

v) Relaxation in maximum age upto 75 years for regular credit cards and/or CIBIL score between 700 to 750 based on existing relationship and account operation is allowed under the sanctioning power of Zonal Manager.

6. Compliance with KYC/AML/CFT /Obligation of Banks under PMLA, 2002

The instructions/guidelines contained in KYC/AML/CFT Policy of Bank dated 23.05.2023 or thereafter should be adhered to in respect of all cards issued. Bank will ensure KYC compliant of any agent, if engaged by the Bank, before engagement.

7. Interest rates and other charges

While determining interest rate on credit card dues, Bank shall consider it in the nature of non-priority sector personal loans.

i) Interest Rate / Finance Charges:

In case the Bank charges interest rates which vary based on the payment/default history of the cardholder, there will be transparency in levying of such differential interest rates.

Bank will upfront indicate to the credit card holder, the methodology of calculation of finance charges with illustrative examples, particularly in situations where a part of the amount outstanding is only paid by the customer. Financial charges like application fee, annual maintenance fee, processing fee etc. (other than interest charges on the outstanding balance beyond due date which shall be approved by ALCO) will be calculated by retail department. All the credit card charges will be got approved from board and will be made as part of existing service charges booklet.

ii) Billing of Credit Card dues:

Credit Card Cell will ensure that there is no delay in dispatching bills and the customer has sufficient number of days (at least one fortnight) for making payment before the interest starts getting charged. In order to obviate frequent complaints of delayed billing, the Credit Card Cell will provide bills and statements of accounts online, with suitable security measures like password protected. Credit Card Cell will also ensure that the customer's acknowledgement is obtained for receipt of the monthly statement.

iii) Flexi pay Facility / EMI Facility on Transactions:

Bank shall provide facility of flexi pay to card holders for making payment above a certain amount of transaction by levying certain processing fee which should be fixed based on cost benefit analysis in consultation with / by retail department and approved by Committee. The customer will be given a minimum number of days within which the customer may apply for this facility. Customers may choose to repay within the block of 3 months i.e. 3/6/9/12/18/24 months. This facility can be availed before/after the transaction is billed on billing date. Transaction done on jewellery/gold purchase will not be allowed for conversion into EMI.

iv) Cash Advance Facility:

Cash advance facility (Withdrawal of Cash through ATM/POS) will be available maximum up to 20% of the total credit limit. There will be no Interest Free Credit period. Also Bank will charge transaction fees (Cash Advance Fees) on each Cash Withdrawal transaction.

Bank will quote **Annualized Percentage Rates (APR)** on card products (separately for retail purchase and for cash advance, if different). The method of calculation of APR should be given with a couple of examples for better comprehension. The APR charged and the annual fee should be shown with equal prominence. The late payment charges, including the method of calculation of such charges and the number of days, should be prominently indicated. The manner in which the outstanding unpaid amount will be included for calculation of interest should also be specifically shown with prominence in all monthly statements. Even where the minimum amount indicated to keep the card valid has been paid, it should be indicated in bold letters that the interest will be charged on the amount due after the due date of payment. These aspects should be shown in the Welcome Kit in addition to being shown in the monthly statement. A legend/notice to the effect that "**Making only the minimum payment every month would result in the repayment stretching over years with consequent interest payment on your outstanding balance**" should be prominently displayed in all the monthly statements so as to caution the customers about the pitfalls in paying only the minimum amount due. The terms and conditions for payment of credit card dues, including the minimum amount due, shall be stipulated so as to ensure there is no negative amortization. An illustration is included in the Annexure I. The unpaid charges/levies/taxes shall not be capitalized for charging/compounding of interest.

v) Most Important Terms and Conditions :

Bank should explain the conversion of outstanding balance and grace period or Interest Free Credit period to the customers. Suitable examples regarding these should be included in the Welcome Kit and on the Bank's website. This should also include terms and conditions for payment of credit card dues, including the minimum payment due. Bank should take efforts on educating the Card Holders about the implications of paying only "The Minimum Amount Due". The MITC should specifically explain that the Interest Free Credit period is lost if any balance of the previous month's bill is outstanding. For this purpose, Bank can work out illustrative examples and include the same in Welcome KIT send to the card holder and place it in on the website.

vi) All the rates of interest for credit card as mentioned above shall be decided by the ALCO as mentioned in the ALM policy. Ceiling for maximum ROI on Credit Card dues shall also be decide by ALCO. ROI note shall be put by Credit Card Cell & place before ALCO for approval through IRM Department.

vii) **Income Recognition Asset Classification:** The past due status of a credit card account for the purpose of asset classification would be reckoned from the payment due date mentioned in the monthly credit card statement. A credit card account should be treated as non-performing asset if the minimum amount due, as mentioned in statement, is not paid fully within 90 days from the next statement date. The gap between the two statements should not be more than a month. Bank will follow this uniform method of determining over-due status for credit card accounts while reporting to credit information companies and for the purpose of levying of penal charges i.e late payment charges, if any.
Upon classification of a credit card account as NPA, to recover the default amount, lien is marked in the related account of the cardholder and to recover the dues the Bank will exercise the right of set-off.
The NPA credit cards where the recovery is not affected despite all-out efforts, the Bank may hand over such cases to recovery Agents/Agencies for recovery of dues.

viii) Any charge that was not explicitly indicated to the credit card holder at the time of issue of the card and without getting his/her consent should not be levied. However, this would not be applicable to charges like GST, etc. which may subsequently be levied by the Government or any other statutory authority.

ix) Changes in charges (other than interest) shall be made only with prospective effect giving notice of at least one month. If a credit card holder desires to surrender his/ her credit card on account of any change in credit card charges to his/ her disadvantage, he/ she should be permitted to do so without levying any extra charge for such closure. Any request for closure of a credit card has to be honoured immediately, subject to full settlement of dues by the cardholder. If Bank decides to issue credit card free of charges for the first year, there will be transparency i.e. without any hidden charges.

7.10 Annual charges are waived.

8. Wrongful billing

i. Credit Card Cell shall ensure that wrong bills are not raised and issued to customers. In case, a customer protests any bill, credit card cell should provide explanation and, if necessary, documentary evidence may also be provided to the customer within a maximum period of 30 days from the date of complaint with a spirit to amicably redress the grievances.

ii. No charges shall be levied on transactions disputed as 'fraud' by the cardholder until the dispute is resolved.

iii. Bank, in order to provide flexibility wrt to billing date, cardholders shall be provided option to modify the billing cycle of the credit card at least once as per their convenience.

iv. Any credit amount arising out of refund/failed/reversed transactions or similar transactions before the due date of payment for which payment has not been made by the cardholder, shall be immediately adjusted against the 'payment due' and notified to the cardholder.

v. Bank shall seek explicit consent of the cardholder to adjust credit amount beyond a cut-off, one percent of the credit limit or ₹5000, whichever is lower, arising out of refund/failed/reversed transactions or similar transactions against the credit limit for which payment has already been made by the cardholder. The consent shall be obtained through e-mail or SMS within seven days of the credit transaction. Bank shall reverse the credit transaction to the cardholder's bank account, if no consent/response is received from the cardholder. Notwithstanding the cut-off, if a cardholder makes a request to the Bank for reversal of the credit amount outstanding in the card account into his/her bank account, the Bank shall do it within three working days from the receipt of such request.

vi. Incorrect interest/charges/penalty/other entries if any wrongly debited to the customer's credit card account shall be reversed with the approval of CM/AGM, Credit Card Cell.

9. Use of Direct Sales Agent (DSAs)/Direct Marketing Agents (DMAs) and other Agents

i. Whenever Bank wishes to outsource any credit card operations, it has to be extremely careful that the appointment of service providers does not compromise with the quality of customer service and Bank's ability to manage credit, liquidity and operation risks. Bank should be guided by the Outsourcing Policy of the Bank and guidelines of RBI issued from time to time / BCSBI's code of conduct as applicable to DSAs and a note regarding this should be approved from the Board before taking the activity.

ii. Bank and any of its third party agent engaged in debt collection process should refrain from actions that could damage the integrity and reputation of the Bank. Strict customer confidentiality should be observed.

iii. All communications issued by recovery agents must contain the name, email-id, telephone number and address of the concerned senior officer of the Bank whom the customer can contact. Further, Bank shall provide the name and contact details of the recovery agent to the cardholder immediately upon assigning the agent to the cardholder.

iv. Bank or its agents shall not resort to intimidation or harassment of any kind, either verbal or physical, against any person in their debt collection efforts, including acts intended to humiliate publicly or intrude upon the privacy of the credit cardholders' family members, referees and friends, making threatening and anonymous calls or making false and misleading representations.

v. Bank shall ensure to comply with the extant guidelines in respect of engagement of recovery agents as per recovery policy of Bank, as amended from time to time.

vi. The disclosure of customers' information to the DSAs/DMAs/recovery agents shall also be limited to the extent that will enable them to discharge their duties. Personal information provided by the cardholder but not required for recovery purposes shall not be released by the Bank. Bank shall ensure that the DSAs/DMAs/recovery agents do not transfer or misuse any customer information during marketing of credit card products.

vii. Bank shall have a system of random checks to ensure that their agents have been properly briefed and trained as to how to handle customers and are also aware of their responsibilities, particularly with regard to soliciting customers, hours for calling, privacy of customer information, conveying the correct terms and conditions of the product on offer.

viii. Bank shall ensure that their employees/agents do not indulge in mis-selling of credit cards by providing incomplete or incorrect information to the customers, prior to the

issuance of a credit card. Bank shall also be liable for the acts of their agents. Repetitive complaints received in this regard against any employee/agent shall be taken on record by the Bank and appropriate action shall be initiated against them including blacklisting of such agents. A dedicated helpline and email-id shall be available for the cardholders to raise complaints against any act of mis-selling or harassment by the representative of the Bank.

ix. Bank shall ensure adherence to the Master Direction DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023 on 'Outsourcing of Information Technology Services' and guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services', as amended from time to time. Further, Bank shall not share card data (including transaction data) of the cardholders with the outsourcing partners unless sharing of such data is essential to discharge the functions assigned to the latter. In case of sharing of any data as stated above, explicit consent from the cardholder shall be obtained. It shall also be ensured that the storage and the ownership of card data remains with the Bank.

Bank will follow the guidelines mentioned below to ensure adherence to **fair practices in debt collection Annexure II.**

10. Collection of Dues

a. Repayment process by way of amount, tenure and periodicity of repayment will be explained to the card holder in advance and acknowledgement for the same will be taken from the customer. However, if the card holder does not adhere to repayment schedule, a defined process in accordance with the laws of the land will be followed for recovery of dues which will be given to the card holder at the time of sanction of credit limit.

b. The process will involve reminding the card holder by sending notice (SMS / Email etc) or by making personal visits.

c. In case of default, Bank may refer the case to the recovery agent. Bank will inform the card holder that recovery proceedings have been initiated.

d. On initiating recovery proceedings Bank will also tell the card holder that in case the card holder is having a complaint to make in this regard he/she may contact Bank's helpline number.

e. Bank will investigate the complaints about unfair practices by recovery agents. In the event of receipt of any complaint from the card holder that the Bank's representative / recovery agent has engaged in any improper conduct or acted in violation of the Code, Bank will investigate the matter and communicate the findings to the card holder within 30 working days from the date of receipt of complaint and wherever justified, compensate the card holder for losses, if any.

11. Policy on Collection of Dues

a. Bank's collection practice should be built on courtesy, fair treatment and persuasion. Bank will foster customer confidence and long- term relationship. As part of Bank's collection practice -

- Bank will provide the card holder with all the information regarding dues and will endeavour to give sufficient notice for payment of dues.
- Bank will write to the card holder when we initiate recovery proceedings against him/her.
- Bank will post details of the recovery agency firms / companies engaged by it on its website.
- Bank will also make available, on request, details of the recovery agency firms/companies at the branches.
- Staff or any person authorized to represent Bank in collection of dues will identify himself/ herself and display the authority letter issued by the Bank and upon request display to the card holder his/ her identity card issued by the Bank.

- Bank will have a system of checks before passing on a default case to collection agencies so that the card holder is not harassed on account of lapses on Bank's part.

b. All the staff members or any person authorised to represent the Bank in collection would be subjected to due diligence and they would follow the guidelines set out below:
   - Card holder would be contacted ordinarily at the place of business / occupation and if unavailable at the place of business/ occupation at the place of card holder's residence or in the absence of any specified place at the place of card holder's authorised representative's choice.
   - Identity and authority to represent would be made known to the card holder at the first instance.
   - Card holder's privacy and dignity would be respected.
   - Interaction with the card holder would be in a civil manner.
   - Normally Bank's representatives will contact card holders between 0700 hrs and 1900 hrs, unless the special circumstances of card holder's business or occupation require otherwise.
   - Card holder's requests to avoid calls at a particular time or at a particular place would be honoured as far as possible.
   - Time and number of calls and contents of conversation would be documented.
   - All assistance would be given to resolve disputes or differences regarding dues in a mutually acceptable and in an orderly manner.
   - During visits to card holder's place for dues collection, decency and decorum would be maintained.
   - Inappropriate occasions such as bereavement in the family or such other calamitous occasions would be avoided for making calls/visits to collect dues.

Part of this Policy (as per regulatory guidelines) will be displayed on the Bank's website and made available on request.

12. Code of Conduct:

Bank and/or any DSA engaged in marketing of Bank's product should strictly adhere to the code of conducts as under.

a. Bank will make sure that all our advertising and promotional material is clear and not misleading.
b. In any advertisement and promotional literature that draws attention to Bank's service or product or includes a reference to an interest rate, Bank shall also indicate whether other fees and charges will apply and full details of the relevant terms and conditions will be made available on request.
c. If Bank avails the services of third parties for providing support services, it will ensure that the third parties handle card holder's personal information (if available to such third parties) with the same degree of confidentiality and security as Bank would.
d. Bank may, from time to time, communicate to the card holder various features of its products availed by the card holder by e-mail, SMS or over the telephone. Information about other products or promotional offers in respect of our products / services will be conveyed to the card holder only if they have not registered for the 'Do Not Call' facility. As regards the information shared through e-mail, card holders have the option to unsubscribe from such future communications.
e. The prescribed code of conduct for Direct Selling Agencies (DSAs) whose services Bank may avail to market its products / services which, amongst other matters, requires them to identify themselves as only selling agents of Bank when they approach card holders for selling our products personally or through phone. Bank shall ensure that any third party or agent acting on our behalf or selling our product complies with the code of conduct.

f. In the event of receipt of any complaint from the card holder that Bank's representative / courier or DSA has engaged in any improper conduct or acted in violation of this Code, Bank shall take appropriate steps to investigate and to handle the complaint and to make good the loss as per the compensation policy of the Bank.
g. Bank shall ensure that any third party or agent acting on its behalf or selling its product discloses the fee or commission they are paid upon completion of the sale.
h. Bank shall ensure that its advertisements will also include all relevant messages which require to be conveyed for enhancing awareness against unscrupulous / fictitious offers.
i. Bank shall run reward program on Credit Card transactions for encouraging customers to enhance Credit Card usage through various promotional offers. These programs can be run by engaging third party Loyalty Reward Companies within the adhered guideline and code of conduct by Bank.
j. The end-to-end activities in respect of Bank's credit card issuance have been outsourced through Request for Proposal (RFP) process for handling various Credit Card Operations and software solutions for Credit Card Business. The service provider is selected for a period of five years after calling RFPs. The service provider and its sub-service providers are PCI DSS (Payment Card Industry –Data Security System) certified. A separate Confidentiality and Secrecy Certificate has been signed with the service provider. Besides above, Bank is also availing services of other service providers/vendors for allied Credit Card business activities like Reward Points Management and Electronic Payment & Collection services etc.

   While outsourcing the various services, it is ensured that it does not compromise confidentiality of the customer's records, respects customer privacy and adheres to fair practices and regulatory guidelines for Credit card industry are adopted. PCI-DSS, PCI-SSF, PCI-PSPE , PCI-PIN certificate etc., wherever applicable, are obtained & kept on record. The outsourced services shall be guided by Bank's Outsourcing Policy and Data Protection Policy.

   Along with the above codes, while engaging third parties, Bank shall take into account all relevant laws, regulations, guidelines and conditions of approval, licensing or registration. Bank shall also ensure that the third parties are properly trained to handle their responsibilities with care and sensitivity particularly in the aspects like soliciting customers, hours for calling, privacy of customer information, conveying the correct terms and conditions of the product on offer, etc. It will also ensure that they do not exceed their brief. Bank will carry out random checking and mystery shopping to ensure these.

   Appointment of third parties should be approved by the Board. Agreement with third party providers should take care of the various activities/responsibilities discussed in above paragraphs.

   Banks shall engage only those telemarketers registered with Telecom Regulatory Authority of India (TRAI) and who comply with directions/regulations on the subject issued by the TRAI from time to time while adhering to guidelines issued on "Unsolicited Commercial Communications – National Customer Preference Register (NCPR)". Bank should periodically check that the engaged telemarketers are not blacklisted by TRAI.

13. Fair Practices Code for Self- Regulation of Credit Card business

The Fair Practices Code incorporates various guidelines on Credit Card issued by RBI from time to time. It also incorporates the principles enunciated in the "Code of Bank's Commitment to Customers" (Code) of The Banking Codes and Standards Board of India (BCSBI). It is the responsibility of the Credit Card Cell to make these codes available on the website and make changes whenever necessary.

14. Issue of unsolicited cards/facilities

Credit Card Cell shall be responsible that unsolicited cards are not to be issued. In case, an unsolicited card is issued and activated without the written consent of the recipient and the latter is billed for the same, the Bank shall not only reverse the charges forthwith, but also pay a penalty without demur to the recipient amounting to twice the value of the charges reversed. Bank will also have to bear any penalty levied by Banking Ombudsman in case the recipient complains about loss of time, expenses incurred, harassment and mental anguish suffered by him.

Any loss arising out of misuse of such unsolicited cards will be the responsibility of the Bank only and the person in whose name the card has been issued cannot be held responsible for the same.

In case of any enhancement in limit, prior consent of the card holder should be obtained as also consent to any changes in terms and conditions. In case of reduction in the credit limit, the Bank shall intimate the same to the cardholder.

15. Customer Confidentiality and Privacy

Bank will treat all personal information of the card holders as private and confidential (even when they are no longer Bank's customer), and shall be guided by the following principles and policies:

15.1. Bank shall not reveal information or data relating to card holder's accounts, whether provided by the card holder or otherwise, to anyone, including other companies /entities in the group without obtaining explicit consent, with regards to the purpose for which the information will be used and the organisation with whom the information is shared, other than in the following exceptional cases:

15.1.1. Providing information to the Credit Information Companies (CICs) as per Credit Information Companies (Regulation) Act (CICA) about the loans, unsecured loans, credit card, etc.

15.1.2. Giving the information required by law or by the Banking regulator.

15.1.3. Fulfilling a duty towards the public to reveal the information.

15.1.4. Bank's interests require it to give the information (for example, to prevent fraud) but Bank shall not use this as a reason for giving information about the card holders or their accounts (including name and address) to anyone else, including other companies in the group, for marketing purposes.

15.1.5. Card holder authorizes Bank to reveal the information.

15.1.6. When required to give a Banker's reference about the card holder, Bank shall need, unless provided earlier, card holder's written permission before it gives it.

15.2. Bank shall not use card holder's personal information for marketing purposes by anyone including itself unless card holder specifically authorizes Bank to do so.

15.3. If Bank collects any information from the card holder other than KYC requirement, it will collect it separately and not as a part of account opening form. In case Bank collects any additional information, it will explain the purpose for which it is collecting this information and take card holder's/applicants specific consent for the same.

15.4. The disclosure to the DSAs/recovery agents should also be limited to the extent that will enable them to discharge their duties. Personal information provided by the card holder but not required for recovery purposes should not be released by the Bank. The Bank should ensure that the DSAs/DMAs do not transfer or misuse any customer information during marketing of credit card products.

15.5. Under a co-branding arrangement, the co-branding entity shall not be permitted to access any details of customer's accounts that may violate the Bank's secrecy obligations.

16. Use of International Credit Card while outside India

Usage of the Card for transacting outside India must be made in accordance with applicable law including the Exchange Control Regulations of the RBI and the Foreign Exchange Management Act, 1999.

17. Transactions which are prohibited using Credit Card

17.1 Remittance of income from racing/ riding etc. or any other hobby.
17.2 Remittance for purchase of lottery tickets, banned /prescribed magazines, football pools, sweepstakes, etc.
17.3 Payment of commission on exports made towards equity investment in Joint Ventures / Wholly Owned Subsidiaries abroad of Indian companies.
17.4 Remittance of dividend by any company to which the requirement of dividend balancing is applicable.
17.5 Payment of commission on exports under Rupee State Credit Route, except commission up to 10% of invoice value of exports of tea and tobacco.
17.6 Payment related to "Call Back Services" of telephones.
17.7 Remittance of interest income on funds held in Non-Resident Special Rupee (Account) Scheme.
17.8 Remittance for carrying transaction with a person resident in Nepal or Bhutan (may be exempted by RBI subject to such terms and conditions as it may consider necessary to stipulate by special or general order).
17.9 Foreign exchange trading through online trading portals.
17.10 As and when the Bank comes across any prohibited transaction undertaken by the credit card customer, the card or the account of the customer will be immediately closed.

18. Transactions which require prior approval of the Central Government

Purpose of Remittance	**Ministry / Department of Govt. of India whose approval is required**
Cultural Tours	Ministry of Human Resources Development, (Department of Education and Culture)
Advertisement in foreign print media for the purposes other than promotion of tourism, foreign investments and international bidding (exceeding USD 10,000) by a State Government and its Public Sector Undertakings	Ministry of Finance, (Department of Economic Affairs)
Remittance of freight of vessel chartered by a PSU	Ministry of Surface Transport, (Chartering Wing)

Payment of import through ocean transport by a Govt. Department or a PSU on c.i.f. basis (i.e. other than f.o.b. and f.a.s. basis)	Ministry of Surface Transport, (Chartering Wing)
Multi-modal transport operators making remittance to their agents abroad	Registration Certificate from the Director General of Shipping
Remittance of hiring charges of transponders by (a) TV Channels (b) Internet Service providers	Ministry of Information and Broadcasting Ministry of Communication and Information Technology
Remittance of container detention charges exceeding the rate prescribed by Director General of Shipping	Ministry of Surface Transport (Director General of Shipping)
Remittance of prize money/sponsorship of sports activity abroad by a person other than International / National / State Level sports bodies, if the amount involved exceeds USD 100,000.	Ministry of Human Resources Development (Department of Youth Affairs and Sports)
Remittance for membership of P&I Club	Ministry of Finance (Insurance Division)

Bank shall ensure capturing transactions where prior approval of Central Government is required.

19. Reporting to Credit Information Companies (CICs)

When a customer applies for credit card facility:

19.1. Bank will explain to the applicant the role of Credit Information Companies (CICs) as also the checks Bank may make with them and the effect that the information they provide can have on the applicant's ability to get credit.

19.2. Bank shall, on request and on payment of the prescribed fee, furnish the applicant a copy of the credit information report obtained by it from the CICs.

19.3. Bank shall provide correct information about credit availed by the card holder to the CICs at periodic intervals.

19.4. Information reported to CICs will also include personal debts of the card holder with Bank when
i. The card holder has fallen behind with his/her payments
ii. The amount owed is in dispute

19.5. Bank shall update the credit status immediately but not later than 30 days on repayment of over dues. Bank shall report closure of loan to CICs within 30 days of the event. If the loan account has been in default, but thereafter regularised, Bank shall update this information with the CICs in the next report. If there is partial / delayed / any settlement of credit dues, it will impact card holder's credit score.

19.6. In case of dispute about the information provided to the CICs, Bank shall resolve the matter by satisfactorily explaining the reasons for reporting to CICs.

19.7. Bank shall, on request, inform the card holder of the details of the CIC(s) to whom Bank submits information regarding the credit / loan facility availed by the card holder from it.

19.8. Bank should follow uniformed method of determining overdue status for Credit Card Accounts while reporting to Credit Information Companies and for the purpose of levying penal charge like late payment charges etc.

19.9 Bank shall report a credit card account as 'past due' to credit information companies (CICs) or levy penal charges, viz. late payment charges and other related charges, if any, only when a credit card account remains 'past due' for more than three days. The number of 'days past due' and late payment charges shall, however, be computed from the payment due date mentioned in the credit card statement. Late payment charges and other related charges shall be levied only on the outstanding amount after the due date and not on the total amount due.

19.10 Before reporting default status of a credit cardholder to a Credit Information Company, the Bank shall ensure that they adhere to a procedure, approved by their Board and intimate the cardholder prior to reporting of the status. In the event the customer settles his/her dues after having been reported as defaulter, the Bank shall update the status within 30 days from the date of settlement. Bank shall be particularly careful in the case of cards where there are pending disputes. The disclosure/release of information, particularly about the default, shall be made only after the dispute is settled.

It should be explicitly brought to the notice of the applicant/card holder that the above information is being provided in terms of the Credit Information Companies (Regulation) Act, 2005.

The above procedures should be part of MITC.

20. Redressal of grievances

a) Bank shall put in place a Grievance Redressal Mechanism within the card issuing entity and give wide publicity about it through electronic and print media. The name, direct contact number, email-id and postal address of the designated grievance redressal officer of the Bank shall be mentioned on the credit card bills and account statements. The designated officer shall ensure that grievances of cardholders are redressed promptly without any delay. Customer grievance to be handled as per Customer service policy of Bank. The grievance redressal procedure and the Bank approved policy shall be displayed on the website of the Bank with a clearly visible link on the homepage. The Grievance Redressal process shall have a provision for automatic escalation of unresolved complaints from a call center/base level to higher authorities. There shall be a system of acknowledging customers complaints for follow up, such as complaint number/docket number, even if the complaints are received over phone.

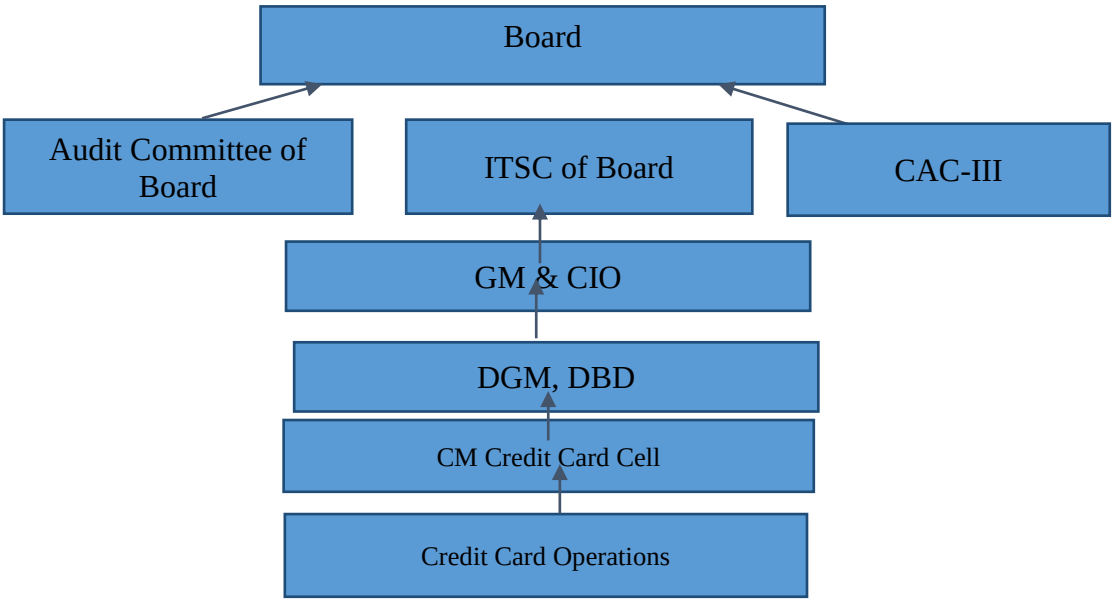
b) All the customer complaints related with Credit Card Cell (including unauthorized transactions and complaints aroused due to act of co-branding partners) will be entered into SPGRS by Customers, call centre staff or branch staff immediately after receiving the customer complaints. The acknowledgement number of customer complaints will be provided to customers through SMS / e-mail for tracking the status of the complaints. The customer grievance will be handled as per bank’s existing customer grievance policy.

c) Bank shall be liable to compensate the complainant for the loss of his/her time, expenses, financial loss as well as for the harassment and mental anguish suffered by him/her for the fault of the Bank and where the grievance has not been redressed in time as per customer service policy of Bank. If a complainant does not get satisfactory response from the Bank within a maximum period of one month from the date of lodging the complaint, he/she will have the option to approach the Office of the concerned RBI Ombudsman for redressal of his/her grievance/s.

d) Customers may refer their complaints/grievances within a time limit of sixty days. It should be given wide publicity by the Marketing division. Frequent training will be

conducted by Credit Card Cell for call centre staff to competently handle all customer complaints.

21. Structure of Credit Card Cell



Credit Card cell will report to Deputy General Manager, Digital Banking Department.

Roles and responsibilities:

a. Underwriting & Card issuance. Card Related operations like hotlisting, limit enhancement. Customer Service, complaints. Credit card promotional activities like running campaigns, followup with branches and zones etc. To prepare and execute strategies for increase of credit card base and transactions. To have tie up with merchant organisations. Audit & compliance related to credit card. SLA monitoring & coordination with service provider.

2. Reconciliation & settlement with interchange (NPCI & VISA). Tie up fintech companies for credit card products. To define and refine customer journey for various process involved in credit card issuance and transaction processing (POS & ECOM). Enhancements in existing products/systems. Implementation of robotic process automation for manual processes involved in credit card issuance, card related operations, reconciliation etc. Digitization of credit card application processing i.e end to end automation from application by customer to delivery of the card to customer.

22. GENERAL GUIDELINES FOR CREDIT CARDS:

i. Bank shall keep internal records to enable operations to be traced and errors to be rectified (taking into account the law of limitation for the time barred cases) as prescribed under ‘Master Direction on Know Your Customer’, as amended from time to time.
ii. The cardholder shall be provided with a record of the transactions after he/she has completed it, immediately in the form of receipt or another form such as the bank statement/email/SMS.
iii. Bank shall block a lost card immediately on being informed by the cardholder.
iv. Any discounts, cashbacks, reward points, loyalty points or any other benefits offered by the Bank shall be provided in a transparent manner including source of such benefits. The accounting process for the same shall be verifiable in the books of the

Bank. Detailed information regarding these benefits shall be displayed on the website of the Bank and a copy of the same shall also be provided to the cardholder.

v. Bank shall provide to the cardholder multiple channels such as a dedicated helpline, dedicated number for SMS, dedicated e-mail-id, Interactive Voice Response, clearly visible link on the website, internet banking and mobile-app or any other mode for reporting an unauthorized transaction on 24 x 7 basis and allow the customer to initiate the blocking of the card. The process for blocking the card, dedicated helpline as well as the SMS numbers, shall be adequately publicized and included in the billing statements.

vi. Bank shall immediately send a confirmation to the cardholder subsequent to the blocking of a card.

vii. Bank shall not dispatch a card to a customer unsolicited. In case of renewal of an existing card, the cardholder shall be provided an option to decline the same if he/she wants to do so before dispatching the renewed card. Further, in case a card is blocked at the request of the cardholder, replacement card in lieu of the blocked card shall be issued with the explicit consent of the cardholder.

viii. In case of an insurance cover provided with a card, Bank shall ensure that the relevant nomination details are recorded by the Insurance Company and the availability of insurance is included, along with other information, in every statement. The information shall also include the details regarding the insurance cover, name/address and telephone number of the Insurance Company which will handle the claims relating to the insurance cover.

ix. The relationship between the Bank and the cardholder shall be contractual. Bank shall make available to the cardholders in writing, a set of contractual terms and conditions governing the issue and use of such cards. These terms shall be expressed clearly and also maintain a fair balance between the interests of the parties concerned.

x. The terms and conditions for the issue and usage of a card shall be mentioned in clear and simple language (preferably in English, Hindi and the local language) comprehensible to the cardholder.

xi. Bank shall not levy any charge that was not explicitly indicated to the cardholder at the time of issue of the card and without getting his/her explicit consent. However, this shall not be applicable to charges like service taxes which may subsequently be levied by the Government or any other statutory authority. The details of all the charges associated with cards shall be displayed on the Bank's website.

xii. The convenience fee, if any charged on specific transactions, shall be indicated to the cardholder in a transparent manner, prior to the transaction.

xiii. The terms shall clearly specify the time-period for reversal of unsuccessful/failed transactions and the compensation payable for failure to meet the specified timeline.

xiv. The terms may be altered by the Bank, but 30 days' notice of the change shall be given to the cardholder to enable him/her to withdraw if he/she so chooses. After the notice period of 30 days, the cardholder would be deemed to have accepted the terms if he/she had not withdrawn during the specified period. The change in terms shall be notified to the cardholder through all the communication channels available.

xv. The terms shall put the cardholder under an obligation to take all appropriate steps to keep the card safe and not to record the PIN or code, in any form that would be intelligible or otherwise accessible to any third party if access is gained to such a record, either honestly or dishonestly.

xvi. The issue of cards as a payment mechanism shall also be subject to relevant instructions on cash withdrawal, issue of international card, security issues and risk mitigation measures, card-to-card fund transfers, merchant discount rates structure, failed ATM transactions, etc, issued by the Department of Payment and Settlement Systems, Reserve Bank of India under the Payment and Settlement Systems Act, 2007, and the Foreign Exchange Department, Reserve Bank of India under Foreign Exchange Management Act, 1999, as amended from time to time.

xvii. **Total Amount Due** is the total amount (net of credit received during the billing cycle, if any) payable by the cardholder as per the credit card statement generated at the end of a billing cycle.

xviii. Interest shall be levied only on the outstanding amount, adjusted for payments/refunds/reversed transactions.

xix. Bank shall provide the list of payment modes authorised by us for making payment towards the credit card dues, in their websites and billing statements. Further, Bank shall advise cardholders to exercise due caution and refrain from making payments through modes other than those authorised by them.

xx. Any debit to the credit card account shall be done as per the authentication framework prescribed by the Reserve Bank from time to time, and not through any other mode/instrument**.**

xxi. For business credit cards wherein the liability rests fully with the corporate or business entity (principal account holder), timeframe provided for payment of dues and adjustment of refunds may be as agreed between the card-issuer and the principal account holder.

xxii. In case Bank, at their discretion, decide to block/deactivate/suspend a credit card, it shall be ensured that a standard operating procedure is followed as approved by their Board. Further, it shall also be ensured that blocking/deactivating/suspending a card or withdrawal of benefits available on any card is immediately intimated to the cardholder along with reasons thereof through electronic means (SMS, email, etc.) and other available modes.

23. Co-branded card:

i. Issuance:

a) Prior approval of the Reserve Bank is not necessary for the issuance of co-branded credit cards by Bank subject to conditions stipulated.

b) The co-branded credit card shall explicitly indicate that the card has been issued under a co-branding arrangement. The co-branding partner shall not advertise/market the co-branded card as its own product. In all marketing/advertising material, the name of the Bank shall be clearly shown.

c) The co-branded card shall prominently bear the branding of the Bank.

d) The co-branding arrangement with Banking/non-banking partner shall be as per Fintech policy and outsourcing policy of the Bank. Further, the information relating to revenue sharing between the Bank and the co-branding partner entity shall be indicated to the cardholder and also displayed on the website of the Bank.

e) Bank shall carry out due diligence in respect of the co-branding partner entity with which they intend to enter into tie-up for issue of such cards to protect themselves against the reputation risk they are exposed to in such an arrangement. Bank shall ensure that in cases where the proposed co-branding partner is a financial entity, it has obtained necessary approvals from its regulator for entering into the co-branding arrangement.

f) Bank shall also be liable for the acts of the co-branding partner. Bank shall ensure adherence to the guidelines as per outsourcing policy of Bank, as amended from time to time. Bank shall ensure that cash backs, discounts and other offers advertised by a co-branding partner are delivered to the cardholder

on time. Bank shall be liable for any delay or non-delivery of the same to the cardholders.

g) Prior approval shall not be required by the banks (all banks including Payments Banks, State Co-operative Banks and District Central Co-operative Banks) and NBFCs registered with the Reserve Bank (NBFCs – ICC, HFC, Factor, MFI, and IFC) to become a co-branding partner of Bank. The role of the co-branding partner shall be as per the conditions stipulated under para 23.

24. Role of co-branding partner

i. The role of the co-branding partner entity under the tie-up arrangement shall be limited to marketing/distribution of the cards and providing access to the cardholder for the goods/services that are offered.

ii. The co-branding partner shall not have access to information relating to transactions undertaken through the co-branded card. Post issuance of the card, the co-branding partner shall not be involved in any of the processes or the controls relating to the co-branded card except for being the initial point of contact in case of grievances. However, for the purpose of cardholder's convenience, card transaction related data may be drawn directly from the Bank's system in an encrypted form and displayed in the CBP platform with robust security. The information displayed through the CBP's platform shall be visible only to the cardholder and shall neither be accessed nor be stored by the CBP.

25. Co-branding arrangement between banks and NBFCs for Credit Cards:

NBFCs, which desire to enter into a co-branding arrangement for issue of credit cards with a card-issuer, shall also be guided by the Guidelines on issue of Co-Branded Credit Cards contained in the respective Master Directions applicable to NBFCs, as amended from time to time.

26. Internal control and monitoring systems

i) The Standing Committee on Customer Services will review the credit card operations including reports of defaulters to a Credit Information Company which has obtained Certificate of Registration from RBI and of which the Bank is a member and credit card related complaints on a monthly basis and take measures to improve the services and ensure the orderly growth in the credit card operations.

ii) The credit card operations shall be guided by the ISSP Policy and Information Security Policy of the Bank.

27. Fraud control – security and other measures

i) Banks shall set up internal control systems to combat frauds and actively participate in fraud prevention committee/ task forces which formulate laws to prevent frauds and take proactive fraud control and enforcement measures.

ii) At the time of issue / re-issue, all cards (physical and virtual) shall be enabled for use only at contact based points of usage [viz. ATMs and Point of Sale (PoS) devices] within India. Bank shall provide cardholders a facility for enabling card not present (domestic and international) transactions, card present (international) transactions and contactless transactions. For existing cards, bank may take a decision, based on their risk perception, whether to disable the card not present (domestic and international) transactions, card present (international) transactions and contactless transaction rights. Existing cards which have never been used for online (card not

present) / international / contactless transactions shall be mandatorily disabled for this purpose.

iii) Bank should also provide
   I. Facility to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic and international, at PoS / ATMs / online transactions / contactless transactions, etc.
   II. The above facility on a 24x7 basis through multiple channels - mobile application / internet banking / ATMs / Interactive Voice Response (IVR); this may also be offered at branches / offices.
   III. Alerts / information / status, etc., through SMS / e-mail, as and when there is any change in status of the card.

iv) Also, international limit should be by default disabled. It should be activated by customer on temporary basis or permanent basis by themselves as per their requirement.

v) Additional factor authentication requirement has been relaxed for values upto Rs.5000/- per transaction for card transactions in contactless mode at Point of Sale(PoS) terminals. Beyond, transactions above Rs.5000/- can be processed using AFA. Also, users to be provided option to switch on/off or to set limits for various card features, including for contactless transactions.

vi) All credit cards will be issued shall be EMV chip and pin based or based on any mechanism that may evolve from time to time.

vii) Bank shall ensure that pin validation is required for every transaction using credit card.

viii) Bank shall ensure that all terminals that accept card swiping should be PCI-DSS (Payment Card Industry- Data Security Standards) and PA-DSS (Payment Applications- Data Security Standards).

ix) Bank shall frame rules based on the transaction pattern of the usage of cards by the customers in coordination with the authorized card payment networks for arresting card related frauds.

x) Fraud monitoring system should be real time basis.

xi) Bank shall immediately hotlist a card on receiving information from customers and formalities including lodging of FIR shall be done within a week. Appropriate insurance coverage in respect of lost cards may be provided to the customers who are ready to bear the cost of premium.

28. Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions

The guidelines issued by the Bank in this regard in Part 1 of para 1.0 Page No. 1 of Customer Service Policy - Compensation Policy for FY 2022-23 should be adhered to.

This policy contains the basic guidelines based on rules and regulations prescribed by RBI and other regulators for carrying out credit card business. When Bank issues a specific credit card there might be some additions required based on the specific feature of that card, requirement of the institution providing platform, Banking scenario at that moment etc. While issuing any credit card Credit Card Cell should put up a note for the Board containing the details of procedures, security and control measures for that specific product based on the guidelines on this policy and as per additional requirement, if any. The note should be vetted by CISO, IRM and then Compliance department before it is put up to the ACB/Board.

29. Audit

Inspection and Audit department, on half-yearly basis, will audit the adequacy and effectiveness of processes and controls for carrying out the operation of credit card and report on this shall be placed before ACB.

30. Review

The policy shall be reviewed on yearly basis.

31. Discontinuation of credit card

If Bank decides to discontinue credit card facility, it will be done by approval of Board.

32. Outsourcing of various services

Bank shall ensure adherence to the Master Direction DoS.CO.CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023 on 'Outsourcing of Information Technology Services' and guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services, as amended from time to time. Further, Bank shall not share card data (including transaction data) of the cardholders with the outsourcing partners unless sharing of such data is essential to discharge the functions assigned to the latter. In case of sharing of any data as stated above, explicit consent from the cardholder Master Directions – Credit Card and Debit Card – Issuance and Conduct Directions, 2022 22 shall be obtained. It shall also be ensured that the storage and the ownership of card data remains with the card-issuer

33. <u>Standard Operating Procedure</u>:

Bank shall issue comprehensive SOP for Credit Card, which shall cover . and FAQs from time to time Limit for staff Credit Card, Application Processing, Upgradation/Limit enhancement of Credit Cards, Benefits & Offers, Most important terms & Conditions, Credit Card Variants etc & FAQ,

34. Conclusion

RBI has the right to impose penalty for violation of its guidelines on credit card business. This policy is based on RBI's Master Circular on credit card.

35. Reference:

This policy is based on

i. RBI Master Direction-Credit Card and Debit Card- Issuance and conduct Directions, 2022 ref no.RBI/2022-23/92 DoR.AUT.REC No.27/24.01.041/2022-23 dated 21st April 2022 Updated as on March 07, 2024.
ii. Reference again from various RBI Guidelines on KYC, AML, Customer Service, Outsourcing etc.

Annexure I

FAIR PRACTICES CODE FOR SELF-REGULATION OF CREDIT CARD BUSINESS

Preamble

This is a voluntary code, adopted by the Bank for the operations of Credit Cards Division. It will act as a benchmark service standard in Bank's dealings with individual customers. The code is expected to help the credit card users in knowing their rights and also measures they should take to protect their interests.

As a voluntary document, the code promotes competition and encourages market forces to achieve higher operating standards to benefit customers. In the code, "you" denotes the credit card customer and "we" denotes the credit card issuer. The standards of the code are governed by the 4 commitments as detailed in Section A.

Unless stated otherwise, all parts of this code apply to all the credit card products and services, whether we provide them across the counter, over the phone, on internet or by any other method.

Commitments outlined in this code is applicable under normal operating environment. In the event of *force majeure*, we may not be able to fulfil the commitments under this code.

A. Key Commitments by the Bank

Bank promises to:

1. Act fairly and reasonably in all its dealings with customers by:
   - Meeting the commitments and standards in this Code, for the products and services that Bank offers, and in the procedures and practices staff/agents follow
   - Making sure Bank's products and services meet relevant laws and regulations
   - Ensuring that our dealings with customers will rest on ethical principles of integrity and transparency.
   - Not engaging in any unlawful or unethical consumer practice.

2. Help customers to understand how Bank's credit card products and services work by giving them the following information in simple language:
   - What are the benefits to customers?
   - How customers can avail of the benefits?
   - What are the financial implications?
   - Whom customers can contact for addressing their queries and how?

3. Deal quickly and effectively with customer queries and complaints by:
   - Offering channels for customers to route their queries
   - Listening to customers patiently
   - Accepting customers mistakes, if any
   - Correcting mistakes/ implementing changes to address customer queries
   - Communicating response to customers promptly
   - Telling customers how to take their complaint forward if they are not satisfied with the response.

4. Publicize this code, by making it available for public access on our website and make copies available for customers on request.

B. Information

Before issuing a credit card to the customer, Bank will

- Explain customers about key features of it, including relevant terms and conditions such as fees and interest charges, billing and payment, renewal and termination procedures and any other information that customers may require to operate the card
- Advice customers about documentation required by the Bank as per regulatory guideline.
- Verify the details provided by the customers

- Explain relevant terms and conditions such as fees and interest charges, billing and payment, renewal and termination procedures and any other information that you may require to operate the card
- Will send a service guide/member booklet giving detailed terms and conditions, interest and charges applicable and other relevant information with respect to usage of credit card along with credit card
- Advise customers of Bank's contact details such as contact telephone numbers, postal address, website/email address to enable them to contact Bank whenever needed.
- If customers do not recognize a transaction which appears on their credit card statement, Bank will give more details on request. In some cases, we may need your cooperation to get us confirmation or evidence that you have not authorised a transaction. If you believe that an error has occurred in the statement you should promptly inform us in writing (so that the same is received by us within 30 days of the date of statement in which the transaction under dispute was charged). The operating rules applicable under the Credit Cards Scheme impose time limits on reporting disputed transactions. If you do not report / inform us within the above time, it would make it difficult for us to gather information about the transactions and this may work to your disadvantage. It is therefore advisable to notify us of any disputed transactions immediately upon receipt of the statement of account.
- Advise customers through Usage guide / MITC of the losses on customers account that customer may be liable if card is lost/misused

C. Marketing Ethics

1. Bank's sales representatives will identify themselves when they approach customers for selling card products. In the event of receipt of any complaint from customer that Bank's representative has engaged in any improper conduct, Bank will take appropriate steps to redress the complaint.
2. If Bank's telemarketing staff/agents contact customers over phone for selling any credit card products or with any cross sell offer, the caller will identify himself/herself and advise customer that he/she is calling on Bank's behalf.

D. Tariff (Fees/Charges/Interest)

1. You can find our schedule of common fees and charges (including interest rates) by:
   - Referring to the Usage guide / MITC
   - Calling up on customer service numbers, or
   - Visiting our website

2. When you become a customer, we will provide you information on the interest rates applicable on your credit card and we will charge the same to your credit card account, if applicable.

3. We will explain how we apply interest to your account on request. However the Most Important Terms and Conditions document and the monthly statements contain details of the method of interest calculation.

4. When we change our tariff (Interest rate or other fees/charges) on our credit card products, we will update the information on our website and monthly statements, and will make the information available at our telephone helpline.

E. Issuance of credit Card / PIN

1. Bank will dispatch credit card to the mailing address/e-mail mentioned by customers through courier / post. Alternatively, we shall deliver your credit card at our branches which maintain your banking accounts(s) under due intimation to you.

2. Green PIN (Personal identification number) needs to be created by card holder himself using OTP on registered mobile number.

F. Account Operations

1. To help customers manage their credit card account and check details of purchase/cash drawings using the credit card, Bank will offer customers a facility to receive credit card transaction details either via monthly mail or through the internet. Credit card statement will be dispatched on a predetermined date of every month.
2. In the event of non-receipt of this information, we expect you to get in touch with us so that we can arrange to resend the details to enable you to make payment and highlight exception if any in a timely manner.

3. We will let you know / notify changes in schedule of fees and charges and terms and conditions. Normally, changes (other than interest rates and those which are a result of regulatory requirements) will be made prospective effect giving sufficient notice.

4. Bank will advise customers what they can do to protect their credit card from misuse.
5. In the event customer's credit card has been lost or stolen, or that someone else knows the PIN or other security information, Bank will, on customer's notifying Bank, take immediate steps to try to prevent these from being misused, subject to operating regulations and law in force.

G. Confidentiality of Account Details

Bank will treat all customer's personal information as private and confidential (even when customers are no longer a customer). Bank will not reveal transaction details of customer's accounts to a third party, including entities in our group, other than in the following exceptional cases

- Providing information to the Credit Information Companies (CICs) as per Credit Information Companies (Regulation) Act (CICA) about the loans, unsecured loans, credit card, etc.
- Giving the information required by law or by the Banking regulator.
- Fulfilling a duty towards the public to reveal the information.
- Bank's interests require it to give the information (for example, to prevent fraud) but Bank shall not use this as a reason for giving information about the card holders or their accounts (including name and address) to anyone else, including other companies in the group, for marketing purposes.
- Card holder authorizes Bank to reveal the information.
- When required to give a Banker's reference about the card holder, Bank shall need, unless provided earlier, card holder's written permission before it gives it.

H. Collection of dues

- Repayment process by way of amount, tenure and periodicity of repayment will be explained to the card holder in advance.
- Bank will investigate the complaints about unfair practices by recovery agents.

I. Redressal of Grievances

1**.** Redressal of complaints internally

- Customers can call Bank's 24-hour call centre numbers or write to Bank or email and Bank's staff will resolve all their queries related to credit card.
- The contacts details are available separately in Bank's marketing collaterals, Usage guide, monthly statements and in the Bank's website.

2. Banking Ombudsman Service and other avenues for redressal

- Within 30 days of lodging a written complaint with Bank, if customer does not get a satisfactory response from Bank and wish to pursue other avenues for redressal of grievances, customer may approach Banking Ombudsman appointed by Reserve Bank of India under Banking Ombudsman Scheme 2006.

J. Termination of Credit Card

1. Any request for closure of a credit card has to be honoured immediately, subject to full settlement of dues by the cardholder. No annual, joining or renewal fees shall be refunded on a pro-rata basis.
2. Bank may terminate customer's credit card, if in Bank's opinion, any breach of agreement is made by the cardholder. Further, it shall be immediately intimated to the cardholder along with reasons thereof through electronic means (SMS, email, etc.) or any other available modes.

K. Scheme guidelines and regulations

All card issuing banks are bound by the regulations of the scheme (Visa, MasterCard and any other scheme under which the card would apply), and in turn you as the customer would be governed and bound by the same. These card operating regulations are subject to changes from time to time by the scheme. We will update you as and when it happens.

L. Feedback and Suggestions

Please provide feedback on our services. Your suggestions will help us to improve our services.

Chapter XV

Robotic Process Automation

1. Aim of this policy:

1.1 Introduction:

The RPA Policy, hereinafter referred to as the “Policy”, is aimed at providing guidance to the users and department of Bank of Maharashtra (hereinafter called the “Bank”), and to lay down the systems and controls expected for Robotics Process Automation.

The policy documents govern the current business strategy of the Bank with regard to Project implementation using RPA in coordination with other department. The policy also lays out the various activities and terms associated with Robotics Process Automation usage.

1.2 Purpose:

RPA tools are software programs designed to interact with existing applications and automate routine rules-based tasks by mimicking user interactions. RPA tools reduce the burden of repetitive, simple tasks on employees, and have the potential to save time and taxpayer dollars, improve accuracy and productivity, ensure standardization and consistency of service, and free employees to focus on more meaningful and analytical work.

Robotic Process Automation is an initiative that would involve automation of critical and highly repetitive Banking processes and also enable reallocation of resources to higher value work efforts to drive better efficiency in the organization.

It will involve identification of critical and highly repetitive processes used in our Bank and automate them by adoption of Intelligent Automation tools in order to reduce human errors, time consumption, manual effort and dependency on resources carrying out tasks.

The scope of RPA in current scenario of our Bank is huge due to the over-dependence on manual workforce to carryout tasks. Adoption of RPA could ensure meeting the following objectives:

- Task Completion without manual intervention or minimal manual supervision.
- Meeting process and project timelines.
- Reducing time taken to execute the tasks.
- Continuous Integration of dependent processes by introducing a pipeline of upstream and downstream jobs.
- Compliance of EASE directives.

1.3 Governance and Intended Audience:

This policy is designed for the concerned departments/Branches who voluntarily participating for testing within the Bank, dealing with products where testing of an application is involved. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank.

The DBD Department shall be responsible for maintaining the implementation of all the procedures involved in Implementation of RPA.

This policy shall be approved by the Board of Directors of the Bank and shall remain valid for a period of one year from such approval/ until reviewed/ policy enforce after one year (in case not reviewed).

2. Formation of RPA Cell

- Automation Team has been formed under Digital Banking Department. The structure of the Cell is as under:

Sl. No.	Designation
01	Assistant General Manager - DBD
02	Chief Manager - DBD
03	Officers – DBD

3. Important Specifications of Robotic Process Automation:

4. Complexity Definitions:

The Bank defines the below sample workflows and the commercials as per the Low-Medium -High complexity definitions of the processes.

5. Process Success criteria for a RPA Process:

Success of the process should be based on one or more the following:

- **Time efficiency**: Template shall mention the time taken in the job/process identified before and after the automation, to establish the time efficiency.
- **Accuracy:** After automation, the accuracy in the result expected.
- **Reduction in manpower / human efforts post automation**.

6. Change Management:

Changes to business applications, IT components and facilities should be managed by change management processes to ensure integrity of any changes. All the IT components proposed under the scope (such as application software, middleware etc.) should be periodically patched for all types of patches, such as - security patches, system patches etc. Emergency patches should also be applied immediately as per regulatory and other agencies directions etc.

If any software provided by Vendor becomes End of support/ End of life during the warranty/ AMC/ ATS period, the same will be replaced by the next version of software without any cost to the Bank. Also, software replacements are done in a planned manner to ensure that no downtime is required on this account.

7. Source Code of the Process:

- The application software should mitigate Application Security Risks, at a minimum, those discussed in OWASP top 10 (Open Web Application Security Project).The Bank shall have right to audit of the complete solution proposed by the Vendor, and

also inspection by the regulators of the country. The Bank shall also have the right to conduct source code audit by third party auditor.

8. User Access Management for RPA Process:

Regular Guidelines for User Access management for Windows user for Vendor should be followed.

RPA Project replicates human activity through BOT Program where it is necessary to provide access through Generic User for various Portals, if required in process flow.

9. Software Requirement on VM Server for RPA Processes:

RPA Project replicates human activities such as operating in Excel, prepare Word Document, read email, send email, copy files, move files, read PDF, read image and prepare report in excel/word/pdf etc. For performing such activity through BOT program on Server, it requires various applications such as MS Office with Email, DB Server, SFTP Server etc. In view of this, the license server based copy should be provided to RPA Project on identified server as per business requirement. Vendor should ask for required software to DBD Team.

10. Security Aspects:

- Conduct regular code reviews to identify and rectify insecure coding practices before deployment
- Continuous monitoring of RPA activities. This includes tracking user activities and changes to workflows or scripts.

11. Standard Operating Procedure:

Bank shall issue comprehensive SOP for Robotic Process Automation, which will include details of User Acceptance Testing, CUG Testing, Roles & Responsibilities, Escalation Matrix and process for all Products.

Chapter XVI

Product Testing

1. Aim of this policy:

1.1. Introduction:

Testing is the process of evaluating a system/service or its component(s) to find whether it achieves the specified requirements or not. In brief, testing is the process of executing a system in order to identify any gaps, errors, or missing in requirements in comparison to the actual requirements.

The process of testing helps in identifying the performance of the system in different circumstances/scenarios and monitoring the behavior of the system. Due to this the performance of any application can be verified and improved at the early stage.

1.2. Governance and Intended Audience:

This policy is designed for the concerned departments/Branches who voluntarily participating for testing within the Bank, dealing with products where testing of an application is involved. The In-Charge, Digital Banking shall be responsible for ensuring that the policy is current with regards to the applicable rules and regulations of the Bank.

The DBD Department shall be responsible for maintaining the implementation of all the procedures involved in testing.

This policy shall be approved by the Board of Directors of the Bank and shall remain valid for a period of one year from such approval/ until reviewed/ policy enforce after one year (in case not reviewed).

2. Important Specifications of Testing:

2.1. Specifications:

Test case objectives: Objectives of an application testing involves the reason or goal for implementing a specific test case.

Test items: These are the documents essential for the execution of a test case. This list of documents includes the User manual, Software Design Document (SDD), and Software Requirement Specifications (SRS), among others. They define the requirements or features that should be met after, during, and before testing.

Test procedure specification: It consists of the step-by-step procedure to run the test case.

Input specifications: The collection of inputs that is essential to run a specific test case with precise values of the inputs and not generalized values.

Output specifications: The design of appearance of the result of a test case implementation. In comparison of the output specifications to the actual outputs to determine the success or failure of a test case. Similar to input specifications, the precise values should be specified.

Environmental Set-up/requirements: The environmental setup for testing the application such as specific platform, devices/tools required etc. should be readily available.

Special procedural needs: These describe the special conditions or constraints essential for fulfilling the test case implementation.

Inter-case dependencies: There are some instances wherein two or more test cases depend on one another for correct implementation. For such instances, the testing team should include these Inter-case dependencies.

2.2. Types of Testing involved in our Projects:

Below are some types of testing involved with our Bank's testing procedures:

i. Regression Testing

Regression testing is a method of testing that is used to ensure that changes made to the software do not introduce new bugs or cause existing functionality to break. It is typically done after changes have been made, such as bug fixes or new features, and is used to verify that the system still works as intended.

The main advantages of regression testing include:

a. It helps to ensure that changes made to the software do not introduce new bugs or cause existing functionality to break.
b. It helps to ensure that the software continues to work as intended after changes have been made.
c. It helps to improve the overall reliability and stability of the software.

* *It's important to keep in mind that regression testing is an ongoing process that should be done throughout the software development*

ii. Alpha Testing

This is a type of acceptance testing which is done before the product is released to customers. It is performed internally within the organization.

iii. System Testing

System Testing is carried out on the whole system in the context of functional requirement specifications. The software is tested such that it works fine for the different operating systems. In this, we have security testing, recovery testing, stress testing and performance testing. This includes both functional as well as nonfunctional testing.

a. **Stress Testing:** Testing the system under unfavorable conditions to check how they perform in those conditions. (Negative Scenarios).

b. **Performance Testing:** It is designed to test the run-time performance like test the speed and effectiveness of the application. It is also called load testing. In this we can test the performance of the system in the given load. (Positive Scenarios)

iv. User Acceptance Testing (UAT)

User department shall perform the UAT for all the products as per the approved test cases to verify the end to end functioning of the application. All issues/ observations raised during UAT should be rectified/closed by the product team and accordingly user department will give UAT sign-off.

v. Beta/CUG Testing

The Beta testing shall be conducted with one or more customers/staffs as the end-user of the service/product. This Beta version shall be released for a limited number of users for testing in a live environment and post successful testing the service/product shall be made live for all the intended customers/staffs.

2.3. Advantages of Application testing:

a. Improved quality and reliability of the system
b. Early identification and fixing of defects
c. Improved customer satisfaction
d. Reduced maintenance costs

3. Procedure involved for testing an application:

i **Requirement analysis:**

The first step of testing an application involves the gathering and analyzing the actual product requirement. In this phase the Business Requirement Document (BRD) from the product owner and Functional Specification document from the partner who design and implement the actual project should be gathered and analyzed thoroughly. Based on this analysis the tester should analyze the feasibility of the testing that can be implemented.

ii **Testing planning:**

Preparation of the Test Plan will be done based on the requirement analysis.
Activities like resource planning, determining roles and responsibilities, training requirements, etc., carried out in this phase. The deliverables of this phase are Test Plan & Effort estimation involved.

iii **Testing design:**

Test case development activity takes place in this phase. Tester prepares test cases, test scripts and test data. Once the test cases are ready then these test cases are reviewed/approved by the higher authorities.

iv **Environment set-up for testing**:

The test environment setup is done based on the requirement list like internal testing for intra-type projects, device based testing for mobile applications etc.

v **Test Execution:**

The test team starts executing the test cases based on the planned test cases. If a test case result is Pass/Fail, then the same should be updated in the test cases. The defect report should be prepared for failed test cases and should be reported to the Development Team for fixing the defects. Retesting will be performed once the defect was fixed.

vi **Test closure:**

The final stage where we prepare Test Closure Report, Test Metrics including both positive and negative scenarios. Test Case Execution report will be submitted in consideration to make sure that there are no high severity defects opened.

4. Compliance with Other instructions

The implementation of testing is subject to relevant instructions and compliances involved in analyzing, testing and verifying the performance of application with in bound to Bank's policies and regulations.

All the projects that are taken up and delivered after testing will be in the state of being in accordance with established guidelines or specifications, or the process of becoming so. Applications that are developed will be in compliance with specifications created by a standards body, and then deployed by user departments in compliance with vendor's licensing agreement.

5. Standard Operating Procedure:

Bank shall issue comprehensive SOP for product testing, which will include details of User Acceptance Testing, CUG Testing for all Products. IT Department shall issue a comprehensive SOP.