



POLICY ON ISSUANCE & OPERATION OF PREPAID INSTRUMENTS (PPI)

I. OBJECTIVE

The objective of the policy is to cover the aspects related to the issuance & operations of the prepaid payment instruments by the Bank encompassing the details related to KYC requirements, limits, safety & security standards, customer protection, grievance redressal etc.

II. SCOPE OF THE POLICY

The policy covers the matter related to issuance of Prepaid Payment Instruments in physical form or virtual form i.e Prepaid Cards and electronic form such as Mobile wallets. The Prepaid instruments issued by the Bank shall be for the domestic usage only.

- a) Aspects related to the issuance of prepaid instruments,
- b) Security and Operational aspects related to PPIs
- c) Types of Prepaid payment instruments, KYC requirement and eligibility
- d) Validity and redemption of PPIs
- e) Deployment of PPIs balances
- f) Refunds in PPIs and Transaction limit
- g) Customer complaint & Grievances redressal

III. APPROVAL FROM REGULATORY AUTHORITY FOR PPI OPERATIONS

As per the Master Direction DPSS.CO.PD.No.1164/02.14.006/2017-18 dated 11th October'2017, no entity can set up and operate payment systems for issuance of PPIs without prior approval / authorization of RBI.

Hence, from the date of the mentioned guidelines, for the issuance of the semi closed and open system PPIs shall be done after obtaining prior approval from RBI.



Bank is presently issuing open loop Prepaid Cards and semi-closed electronic mobile wallet. However, in case of Semi-closed electronic mobile wallet, bank doesn't permit any new registration of the user.

IV. POLICY FRAMEWORK

A. DEFINITIONS

1) 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. Our Bank is presently issuing following category of PPIs:

a) Semi-closed System PPIs (Mobile Wallet)

These PPIs can be used for purchase of goods and services only, at a group of clearly identified merchant locations / establishments/ online merchants (or contract through a payment aggregator / payment gateway) to accept the PPIs as payment instruments.

b) Open System PPIs (Prepaid Cards)

The Prepaid Cards issued by the Bank is classified as 'Open System PPIs' as they can be used at any merchant for purchase of goods and services as well as also facilitate cash withdrawal at ATMs / Point of Sale (PoS) / Business Correspondents (BCs).

2) Limits

The maximum limit of Prepaid Cards issued by the Bank has maximum daily loading of ₹10,000/- with maximum monthly limit of ₹25,000/- not exceeding balance of ₹50,000/- at any point of time and subject to maximum annual cumulative credit of ₹2.00 Lac. The maximum limit as well as cumulative limit in the mobile wallet is capped at ₹10,000/- per month. However, presently Bank doesn't allow credit or loading of the Mobile wallet. The users can only consume the money already available in the mobile wallet.

3) 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.



The following definitions have been included in the policy document with respect to the Prepaid Cards either in physical or virtual form issued by the Bank to the customer:

4) Card Number

At present our Bank issues Cards with 16 digit number printed on Debit/ Prepaid Cards. First 6 digits represent Bank's identification no., next 2 digits represent product code and remaining digits indicate serial number of the cards.

5) Card Verification Value (CVV/CVV2)

Card Verification Value is a Three (03) digit number printed on the reverse/back side of every debit/ prepaid card. The CVV is used for validation of online transactions.

6) Expiry Date/ Valid Thru Date

The Valid Thru Date or Expiry date is written on the Face/ Front/ Fascia of the Card in the MM/YY format indicating the validity of the Card. The card is valid till the last day of the mentioned month. The valid thru date/ Expiry date is also being used for validation of online transactions.

7) Magnetic Strip

Magnetic strip is available on the reverse/ back side of the Card which carries important information regarding card in electronic format. Any kind of scratches or exposure to magnetic fields will cause damage to the card.

8) EMV Chip Card

EMV stands for Europay, MasterCard and Visa, which provides the global standard for credit, debit and prepaid cards payment based on chip card technology. The EMV chip is present on the fascia/ face of the card containing important details in the encrypted format. EMV Chip Card protects against counterfeit (skimming) card fraud.

9) Cardholder data

Cardholder data is any personally identifiable data associated with a cardholder. Examples include but are not limited to the primary account number, Card number, cardholder name, expiry date, CVV, PIN, OTP (One Time Pin) etc. The card credentials are personal information which must be protected by the customer and customer has to always undertake reasonable security to not share/ disclose such credentials with any other party.



10) Card association

A card association is a network on which the Card issuing Bank has issued the Card, which facilitates the processing of the Cards through acquiring banks and which are associated with the of issuing banks and acquiring banks that process payment cards of a specific brand.

Internationally, at overseas locations, Card can be used at only those locations wherein the Card association 'Logo' is displayed (*present on fascia of the card*) or Card association partner brands 'Logos' are displayed, which has been provided on the reverse/ back of the Card

11) PIN (Personal Identification Number)

PIN is a FOUR (04) digit code/ number referred to as the Personal Identification Number (PIN) which is assigned by the Bank to the cardholder for validation of ATM/ POS transactions as second factor of authentication (2FA). The Cardholder will be required to enter his/her PIN to avail of the ATM/ POS services using the card. In case of physical PIN mailer sent by the Bank, the Cardholder is required to ensure that the PIN mailer is not tampered and change the PIN immediately at the nearest Bank's ATM.

12) Green PIN

GREEN PIN refers to paperless and instant generation of Personal Identification Number (PIN) for Debit Cards through a self-service option for Debit Card holders. The customer can generate their new PIN or reset PIN for Banks Debit Cards on their own by using OTP sent on their registered Mobile Number. For new cardholders, no PIN is sent to customer in case their mobile number is registered with the Bank and such customers can generate their PIN on their own using 'Green PIN' option on Bank's ATMs.

13) OTP (One time Password)

OTP is a six digit dynamic PIN provided to the customer for authentication of the eCommerce transactions which is valid for one transaction and for a specific period of time. The OTP is sent on the Registered Mobile Number (RMN) of the customer and the same must not be shared by customer to any third party including Bank Staff.

14) POS terminal

A point of sale terminal (POS terminal) is an electronic device used to process card payments at retail locations. The Card terminals provide priority



to chip for card authentication wherever chip cards are presented. The authentication of the transaction is being done using PIN, which is same as ATM PIN.

15) Payment Gateway

The payment gateway facilitates online/ eCommerce payment without physical presence of the Card. The transaction is facilitated through Card number, expiry date and CVV as card credentials along with dynamic OTP (One Time Password) for transaction validation. The online payment can also be facilitated through Direct Debit & PIN combination.

However, for international transaction, only card credentials i.e. Card number, Expiry date and CVV is required for completion of the international online transaction.

16) Card Present Transactions (CP)

The payment transactions requiring physical presence of the payment instruments at the point of transactions shall be classified as CP/Face-to-Face/ Proximity payment transactions. *Eg: Payment transactions initiated through Card at ATMs or at Business Correspondent (BC/ POT), Card at POS including swipe/ dip of card, tap & go payments, NFC (Near Field Communication) based payments, Card linked QR based payments etc.*

17) Card Not Present Transactions (CNP)

The remote/ online payment transactions which doesn't require the physical presence of the payment instrument at the point of transactions are CNP. *Eg: Payment transactions undertaken using Card (Debit/ Prepaid) on eCommerce platform or payment gateway, link based payments etc.*

18) ATM (Automated Teller Machines)

ATM are machines deployed by the Banks and participating institutions (such as White Label ATM Operators, as licensed by RBI) to operate the ATM outlet. The customer shall primarily use the ATM machines to withdraw cash by using their Cards.

19) Micro ATM or POT machines

Micro Automated Teller Machines are POS like machines used by Business correspondents (BC) and Business Facilitators (BF) attached to any bank, wherein they carry the micro ATM as handheld devices for facilitating Banking transactions.



BC/ BF will facilitate the Cardholders at villages/ remote places/ urban locations etc. to provide accessible banking facilities for cash withdrawal (*upto prescribed limit per day*), cash deposits, balance enquiry etc. The BC / BF machine also facilitates Aadhaar based transaction including account opening, cash withdrawal, cash deposit etc.

20) Chargeback

Chargeback is the procedure for registering the dispute with the Bank (Card Issuer) by the Cardholder for the transactions disputed by the customer due to double debit/ failed transactions etc. The customer is required to fill the chargeback form and submit to any branch of OBC.

21) Unauthorized transactions

Unauthorized/ fraudulent transactions on Cards are such transactions which have not been authorized by the customer through specified process of authentication on respective channels. However, these transactions have been effected in the customer's Card/ account by way of contributory negligence on the part of customer by sharing payment credentials, negligence/ deficiency/ contributory fraud ascertained on the part of Bank or due to a third party breach wherein the deficiency lies neither with the Bank nor with the customer.

B. BRIEF ON SAFETY & SECURITY MEASURES

Bank has implemented robust system for safeguarding the access to Card and online/ electronic payment instruments by maintaining Payment Card Industry Data Security Standards (PCIDSS) and Information Security Standards (ISO 27001: 2013).

The Prepaid Payment Instruments offered by the Bank to the customers shall be governed by the Information Security Policy of the Bank and the guidelines issued by the RBI from time to time in the said matter.

The security standards have been adopted by ensuring a balance between security and customer convenience. The transactions are authorized using 2 Factor of Authentication (2FA) for Card based transactions, which is briefed as under:



Prepaid Cards: In the proximity based transaction or Card Present Transaction using Prepaid cards at ATM (if permitted for cash withdrawal) or POS (Point of sales machine), the transactions are authorized using input of PIN by the customer.

The customer shall at all times safeguard the physical card and PIN. However, for eCommerce transactions (domestic), the customer is required to input Card credentials i.e. Card number, expiry date & CVV and then input the dynamic OTP (One Time Password) received on the registered mobile number for authorizing the transaction, which is valid for one transaction only.

Also, the customer's Card credentials to an extent of Card number (Masked) and expiry date is stored by payment gateway (for registered users), wherein the customers are required to input the CVV number and OTP only for authorizing the transaction.

However, for online/ eCommerce international transaction, only card credentials i.e. Card number, Expiry date and CVV is required for completion of transaction.

The Prepaid Cards thus issued are either in physical or virtual form and can only be used for domestic purpose.

Security measures for electronic Prepaid Payment Instruments

- a) The compliance of the measures of the Cyber security policy of the Bank is to be done for Prepaid Payment Instruments.
- b) The Bank shall be the responsible for the losses incurred by any party on account of breach of security or failure of the security mechanism attributable to the Bank.
- c) The customer shall be responsible for the loss due to sharing of customer credentials, card credentials, PIN/ OTP etc.
- d) The cardholder shall be provided with the alerts of the transaction to their Registered Mobile Number.
- e) The customer/ cardholder can at any time of the day or night notify the loss, theft or copying of their payment devices by contacting the Bank's Customer Care 24*7 (Toll free- 1800-180-1235, 1800-102-1235 & Tolloed no. 0120-2580001).
- f) On receipt of notification of the loss, theft or copying of the card, the bank shall block the Card to restrict any further misuse of the Card.



C. ISSUANCE OF PREPAID PAYMENT INSTRUMENTS

i. PREPAID CARDS

Prepaid cards shall be issued to individual customers as well as 'entities / employers' such as Listed Corporate/ unlisted corporate / partnership firms / sole proprietorship / public organizations like municipal corporations, urban local bodies, etc. (employers) for onward issuance to prepaid cards to their staff / employees / contract workers, etc.

The Oriental Prepaid Card shall be provided as 'Ready kit' which can be issued to the individual customers as well as entities/ employers under the specified schemes.

- The prepaid card shall be issued for 'Domestic' purposes only in Rupee denominated cards. The Prepaid Card cannot be issued to NRE/ NRO customers and foreign nationals.
- The facility is to be extended only to those entities/ 'employers' that have a fully KYC compliant existing operative bank account with our Bank. Entities/ Employers/ Corporate Customer are allowed to purchase the Prepaid Card for themselves such as transport operators, office expenses card etc. and/ or in bulk for their employees/ labourers/ beneficiaries etc. as payroll cards after completing the Application process.
- For the individuals, the prepaid card shall be issued after completing the **Full KYC** of the customer. Hence, the Prepaid Cards are issued under the scheme with KYC Due Diligence (KYD) having Separate Account Opening Form (AOF) along with merged Customer Identification Form (CIF). UCIC (Unique Customer Identification Code) provisions shall be applicable for the Prepaid Card scheme.
- The individual purchasing the Prepaid Card shall declare the end-beneficiary in case the card is purchased for someone else. Otherwise, the individual applying for the prepaid card will be considered as end-beneficiary.
- Prepaid Card scheme can also be availed & operated by Minors above the age of 14 years with standard Full KYC only. Further, on minor attaining the age of majority, the account shall not be made "freeze". However, the mentioned scheme shall not be available for Minors with operations mode "Account operated by Guardians".



- Prepaid Card shall be used for only ATM cash withdrawal, POS & e-Commerce transactions and cash withdrawal at BCs.
- The Prepaid Card shall be valid for a minimum period of **03 (three) years**, subject to the **expiry date mentioned on the fascia of Card.**
- The Credit to the prepaid card account shall be permitted either through (1) Cash or (2) OBC Bank account transfer (self A/c) only. *(In case of 'Entities/ Employers' Cash mode for loading of prepaid Card is not permissible).*
- To close the Prepaid card the customer has to surrender the card and request the branch to close the prepaid account. The branch will be required to close the prepaid card upon receiving such request and then proceed with the closure of the account after taking possession of the card. The unutilized balance shall be transferred to the KYC compliant account maintained with the bank of the same customer. The charges shall apply as per the charges schedule for the same.
- No interest shall be payable on the balances transferred to prepaid cards.
- The customer is required to submit a duly filled application form along with acceptance of applicable Terms & conditions for the issuance of the Pre-paid cards.

As to the extent of the policy, only Online Prepaid cards shall be issued by the Bank i.e. transaction initiated by Prepaid cards shall be undertaken through direct connectivity with the Banks system and not through the network option for offline cards.

Bank issues Cards under RuPay branded Non-personalized Prepaid Cards, which are as under:

- Prepaid Cards for Individuals (RuPay)
- Prepaid Cards for Corporate (RuPay)

Bank is presently issuing following variants of the Cards for the customers:

Card Variant	Daily withdrawal limits (ATM and POS or e-Commerce)	Supported in networks
RuPay Prepaid Card	₹10,000/- each	NFS & RuPay (Domestic only)

**NFS- National Financial Switch*



ii. **ELECTRONIC PREPAID INSTRUMENTS (Mobile Wallet)**

Bank has presently issued PPIs upto ₹10,000/- with minimum details of the PPI holder i.e. Name, Date of Birth, Mobile number, E-Mail ID etc. along with mobile number verified with One Time Pin (OTP). However, with effect from 01.01.2018, No customer can subscribe to the electronic PPI issued by the Bank. Only existing users can use the PPI wallet to the extent of the balances available.

D. VALIDITY AND REDEMPTION OF PPI

All PPIs issued by the Bank shall have minimum validity period of one year from the date of issuance / last loading / reloading in the PPI, as applicable, which shall be communicated in advance to the customer at the time of issuance.

For the prepaid cards the validity period shall be mentioned on the card, and then the customer shall have the option to seek replacement of the card upon expiry of the card. The PPI holder shall be intimated before 45 days from the date of expiry, notifying the expiry of the Prepaid Payment Instrument.

PPIs with no financial transaction for a consecutive period of one year shall be made inactive by the bank after sending a notice to the PPI holder/s. These can be reactivated only after validation and applicable due diligence. These PPIs shall be reported to RBI separately. 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.

Upon the expiry of the PPI, the monies left in the wallet shall be handled in accordance to “The Depositor Education and Awareness Fund (DEAF) Scheme, 2014, Section 26A of Banking Regulation Act, 1949” and Banks “Policy on Classification of Inoperative/ Dormant accounts and unclaimed deposit”.

E. COMPLAINTS/ GRIEVANCES REDRESSAL

All the important terms and conditions shall be explicitly informed to the customer in clear and simple bilingual language, as applicable, to the holders while issuing the instruments.

These disclosures shall include:

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



- c. Display Frequently Asked Questions (FAQs) on website / mobile app related to the PPIs.

In case of grievances, the customer shall contact Bank's customer care and Internal Ombudsman of the Bank for resolution of their complaint. The information regarding the same shall be made available on the Banks website for customer access. The customers shall have recourse to the Banking Ombudsman Scheme for grievance redressal. All the grievances raised by the PPI holders shall be endeavored to be resolved within 48 business hours and not later than 30 days from the date of receipt of such complaint/ grievance.

F. REPORTING OF UNAUTHORIZED TRANSACTION BY CUSTOMERS TO BANK

Bank sends alerts through SMS to the customers on their registered mobile number for the financial transactions undertaken by them in their accounts using the electronic channels.

The SMS alerts shall be mandatorily sent to the customers having registered mobile number. The customers are required to inform or notify the Bank about the unauthorized/ fraudulent transactions upon receipt of such alerts.

Further, in case of unauthorized transaction through Prepaid Card or PPIs, the liability of the customer shall be in accordance with the Bank's Compensation Policy- 'E-Channels for Unauthorized/ Fraudulent Electronic transaction'.

G. OPERATIONAL ASPECTS

- a) **Issuance of Duplicate Prepaid Card (Physical) on account of lost or Damaged**

On receiving a 'lost/damaged card' complaint from the customer over telephone (Customer Care) or physically in the branches, the card status will be changed to 'Hot' within 30 minutes.

The customer request for the new card request shall be updated by the branch after closure of the 'Lost/ damaged card' and issuance of the new prepaid card along with transferring the remaining balance to the newly issued prepaid card.



b) Handling Duplicate/ Lost PIN Mailer- Prepaid Card (Physical)

In case of a requirement of PIN due to ‘Duplicate/ Lost PIN Mailer’, customer shall be required to place request for physical PIN at card issuing branch. New PIN Mailer shall be issued and dispatched through courier/speed post to branch for onward delivery to the customer under proper acknowledgement.

However, customer can alternatively avail the facility of ‘Green PIN’ on Bank’s ATM for the generation or re-generation of PIN.

c) Transaction Limit & Other Charges

Transaction limit and other charges are as per the discretion of the bank and guidelines of Regulatory Authorities subject to revision from time to time. The charges related to the Cards are being published by the Bank.

d) Lost or Stolen Report- Prepaid Card (Physical)

If any Customer’s card is lost or stolen or if PIN is disclosed to a third party, customer has to report the incident immediately by calling Customer Service Hotline at Bank’s Customer Care 24*7 (Toll free- 1800-180-1235, 1800-102-1235 & Tolled no. 0120-2580001).

Customer is liable for all amounts debited to account using Prepaid Card as a result of the unauthorized use of card/PIN/OTP until reported loss, theft or disclosure of your card or PIN. If card/PIN which has been reported lost or stolen, is recovered, it must not be used again.

The card holder shall bear the loss sustained up to the time of notification to the bank in case 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 to make the card “HOT” within 30 minutes.

H. INTEROPERABILITY

The Prepaid Cards issued by the Bank offers interoperability wherein users are seamlessly able to use their Prepaid Card on ATM/ POS/ eCommerce. The Mobile wallet issued by the Bank is semi-closed and doesn’t allow interoperability.
