UPI Consolidated Circular

Version 1.0

UNIFIED PAYMENTS INTERFACE

Date of Issue

18th September 2026

VERSION HISTORY

Sr No.	Version Number	Revision History	Date of Release
1	V 1.0	UPI Consolidated Circular	18/09/2026

Contents

PART I: PRELIMINARY

1. Scope & Applicability

1.1 National Payments Corporation of India (NPCI), as the authorised payment system operator of Unified Payments Interface (UPI), under the Payment and Settlement Systems Act, 2007 (PSS Act, 2007), is issuing the UPI Consolidated Circular (hereinafter referred to as "Consolidated Circular").

1.2 The rules, regulations, terms and conditions embodied herein shall govern the operation of participation in and access to UPI.

1.3 This Consolidated Circular shall be applicable to all Members, UPI Application Providers and other system participants of UPI, based on the nature of their participation in UPI. This Consolidated Circular shall be adhered to, and complied with, by each Member, UPI Application Provider and other system participants of UPI.

1.4 This Consolidated Circular incorporates and combines the UPI Operating Circulars issued up to July 31, 2026.[1] All such Operating Circulars shall continue in substance, effect, be applicable and read in consonance with this Consolidated Circular until the same are withdrawn by NPCI. All Operating Circulars listed in Annexure G stand withdrawn by NPCI with immediate effect.

1.5 UPI Procedural Guidelines (UPI PG), Operating and Settlement Guidelines (OSG), Technical Specification Documents (TSDs), Operating Circulars, Risk Management Directions (RMD), NPCI and UPI Brand Guidelines, UPI Information Security Compliance Framework, Error and Response Codes Document, UPI Application Providers checklist, Product Feature Document, Operating Circulars related to Pricing, UPI API usage guidelines and monitoring framework issued by NPCI shall continue to be in effect, be applicable to and shall be adhered to by the Members, UPI Application Providers and other system participants of UPI.

1.6 The provisions of this Consolidated Circular shall be in addition to, and not in derogation of, the provisions of the PSS Act, 2007 and other extant Applicable Laws. Members, UPI Application Providers and other system participants shall comply with the extant Applicable Laws in the course of their participation in UPI. In the event of any conflict between Consolidated Circular and any Applicable Laws, the relevant Applicable Laws shall govern and prevail.

[1] Consolidated Circular does not alter any fee, charges, effective date, compliance timeline or technical requirement stated in Operating Circulars issued up to July 31, 2026.

Part II: UPI OVERVIEW, PARTICIPATION, ROLES AND RESPONSIBILITIES

UPI is an interoperable, real-time payment system developed and operated by NPCI, that provides a standardized API-based framework and specifications for seamless digital payments. UPI offers a single platform that allows its Members and other system participants to process payment instructions and related transactions of their respective Users, including but not limited to, send and receive payments / funds, make merchant payments, manage Mandates, and access various payment features/ services.

NPCI, as the authorised payment system operator of UPI, offers a standardised API based system / framework and processes payment transactions of the Member and UPI Application Provider as per the payment instructions received by it from such system participants. NPCI is responsible for transaction processing, clearing and settlement of payment instructions between the Members and other system participants. The Members, UPI Application Providers and other system participants, in turn, offer UPI-based payment services and features/ services to their Users, thereby enabling such Users to undertake real time payment transactions. Members and system participants independently choose to utilise the UPI payment system for processing payment transactions undertaken / initiated by their Users, in accordance with the features and services supported by UPI.

The widespread availability of and access to UPI features/ services for Users depend on such features/ services being enabled by Payment Service Provider (PSP) and third parties associated with them without undue restrictions. Accordingly, all UPI features/ services enabled by PSPs or third parties associated with them shall be interoperable in nature and made available in the manner that promotes broad-based adoption across the UPI ecosystem.

2. Participation in UPI

2.1 Bank, including Regional Rural Bank, Co-operative Bank, Urban Co-operative Bank, Payments Bank, having a valid license to conduct the business of banking in India and having a valid mobile banking license, can participate in UPI. A Bank can participate either as a direct Member or Sub-Member and as a Remitter, Acquirer, Beneficiary Bank and / or PSP. PPI Issuer having a valid license to issue Prepaid Payment Instruments (PPIs) can participate in UPI as Member or Sub-Member and as an issuer and PSP. Non-Banking Financial Company having a valid registration certificate to carry out financial and lending business operations in India can participate in UPI as a Sub-Member and as an issuer and Beneficiary Bank.

2.2 Member, UPI Application Provider and other system participant must comply with, and ensure compliance with, the UPI System Requirements. Member, UPI Application Provider and system participant shall further ensure that all other system participants for which they are responsible under the UPI System Requirements, including participant or entity connected or interacting with, the User directly or indirectly for or on behalf of such Member or UPI Application Provider, comply with and adhere to the UPI System Requirements. Member shall be guided by extant regulatory guidelines on Additional Factor of Authentication (AFA).

2.3 Each UPI Application Provider shall have and maintain a unique application identification (App IDs) for each of its UPI-based applications across different operating systems, to enable clear segregation and identification of operating system-specific actions, requirements or obligations that may arise from time to time.

2.4 UPI Application Provider shall ensure that its UPI Application can read both UPI QR codes and Bharat QR codes.

2.5 UPI Application Provider shall respond to an Intent call initiated by a Merchant's application only where the User has been registered on, and has set a UPI PIN for, that UPI Application, unless the User has been registered as a Secondary User under UPI Circle.

2.6 UPI Application Provider shall ensure the details of the transactions (amount, beneficiary name, among others) are displayed to the User before transaction authorization. This shall be an additional step before the UPI Common Library (CL) is invoked for authentication.

2.7 PSP and UPI Application Provider shall certify and ensure minimum 1.8 UPI CL version.

2.8 PSP and UPI Application Provider shall adhere to the UPI Deep Linking URL Specifications, including UPI QR and Intent standards, issued by NPCI and as amended from time to time. Payee PSP shall ensure that all mandatory fields and correct values are passed in accordance with the applicable specifications, Payer PSP and UPI Application Provider shall ensure that such values are not altered, except where expressly permitted.

2.9 Payer PSP/UPI Application Provider shall ensure that if there is a device change for an existing User (such as change of handset, re-installation of the UPI Application, among others) and the new device is on iOS operating system, the User shall again set the UPI PIN using the existing UPI PIN set methods (debit card, Aadhaar OTP, UIDAI face authentication, or any other methods introduced from time to time), even if the User uses the same UPI Application Provider on the changed/new device. Additionally on the changed/new device, UPI LITE shall be allowed/activated only after completion of UPI PIN set process.

2.10 Third Party Application Provider (TPAP) with a monthly transaction volume market share exceeding 5% shall integrate with more than one PSP under the multi-bank model subject to a maximum limit of ten (10) PSPs.

2.11 TPAP live on multi-bank model shall ensure that the User is allocated the handle of the bank with which the User has their bank account. For all other Users, TPAPs to ensure that handle allocation through a fair (equal distribution) handle allocation. TPAP operating under the multi-bank model shall submit the month-wise handle allocation report by April each year, covering the preceding financial year.

2.12 UPI Application Provider shall provide an option of enabling/revoking User's location access/permission. UPI Application Provider shall capture User's location only post consent from User as per Applicable Law and the same will be revocable. UPI services shall not be disabled in case location related consent is not provided/ revoked by User. This rule shall be applicable to a User in domestic transactions only.

2.13 For transactions initiated using UPI ID, UPI Number or Account Number and IFSC, the Payee PSP/ Beneficiary Bank shall ensure that the Beneficiary's Core Banking System (CBS) name is conveyed, and Payer PSP/UPI Application Provider shall ensure that the same is displayed to the User for verification before transaction initiation and also displayed in transaction statement/history.

2.14 For Merchant transactions, the Payee PSP shall convey the identity of the end Beneficiary for every transaction. For Verified Merchants, the validated brand name of the Merchant shall be conveyed and for non-verified Merchants, either the CBS name or the validated brand name shall be conveyed. Where the Merchant transaction involves credit to a User's account on an aggregator platform, including credit card payments, NETC recharge, wallet payments, among others, the end Beneficiary shall be identified as the registered name for such User.

2.15 UPI Application Provider shall ensure that names captured from QR codes or User-defined names are not displayed as the Beneficiary's name for transaction purposes. UPI Application Provider shall disable any option that allows Users to modify the Beneficiary's name for transaction purposes.

2.16 PSP and UPI Application Provider shall ensure that 'collect' functionality on Person-to-Person (P2P) transactions is not permitted.

3. User Onboarding and Activation

3.1 Users may access UPI through a UPI Application by linking their account or a permitted payment instrument such as savings account, current account, overdraft, among others.

3.2 Payer PSP and UPI Application Provider shall ensure that the new User registration process on the UPI Application, including device binding, account selection and linking, UPI ID creation, and UPI PIN setup, is carried out in accordance with UPI System Requirements.

3.3 UPI Application Provider shall ensure that a UPI PIN is set for the linked account through the applicable UPI PIN setup methods, including debit card details, Aadhaar OTP, Aadhaar face authentication or any other method introduced from time to time prior to initiating UPI payments. Member shall ensure it adheres to the Applicable Laws and any guidelines, directions and notifications issued by UIDAI and other competent authority for using Aadhaar based authentication.

3.4 Payer PSP shall be responsible for the first factor of authentication, including device binding, application security, the secure generation of tokens (at the device binding stage) and the dynamic Credblock Value (at the transaction stage).

3.5 Remitter Bank shall be responsible for UPI PIN authentication or for validating nonce-based challenge / authentication in cases involving biometric authentication (fingerprint, face, among others) and account-level authorisation.

4. Virtual Payment Address (UPI ID) Creation, Management and Security

4.1 A UPI ID is a unique identifier (e.g., username@pspname) issued and assigned by a PSP to a User or Merchant for sending or receiving UPI payments.

4.2 PSP/UPI Application Provider shall support the creation of both mobile number-based (identified at the time of device binding) and non-mobile number-based UPI IDs, in accordance with the rules and regulations applicable to UPI, and permit Users to set any UPI ID as their default UPI ID.

4.3 In compliance with data privacy requirements as applicable, each PSP shall ensure that UPI IDs are created in a manner that minimizes the exposure of sensitive User information and complete account numbers, card details, or other confidential User identifiers shall not be used in UPI IDs. Where User-related references are required for business convenience, such details shall be masked, truncated, tokenized, or combined in a manner that does not directly disclose sensitive information. The Payer and Payee PSP shall each be responsible for ensuring appropriate safeguards in case of misuse arising from the information embedded in the User and Merchant UPI IDs, respectively.

4.4 PSP/UPI Application Provider shall ensure that Users and Merchants are not permitted to create misleading UPI IDs on any UPI Application.

4.5 UPI Application Provider shall ensure that a secondary/back-up UPI ID is permitted for a multi-bank model UPI Application to improve User experience and to route transactions only when the original (primary) PSP is unavailable due to technical reasons. As soon as the primary PSP is available, the User shall be restored to the primary UPI ID for all UPI transactions.

4.6 UPI Application Provider shall ensure that the secondary/ back-up UPI ID is created with the consent of the User and that it includes a de-registration option. The PSP shall comply with the UPI System Requirements for device binding while creating a secondary/ back-up UPI ID.

4.7 Mobile Numbers, UPI IDs containing mobile numbers and account numbers shall be masked (with only the last four digits visible) across all User-facing interfaces and communications. A User’s own UPI ID shall be masked but an option shall be provided to view or copy the clear UPI ID whenever required.

4.8 Members shall not permit transactions where the remitter and beneficiary accounts are the same.

5. UPI Number

A UPI Number (Numeric UPI ID) is a numeric payment identifier that a User may voluntarily set up against their existing UPI ID (Username@PSP), enabling the User to send and receive payments.

5.1 UPI Application Provider shall permit the User to set a UPI Number comprising either: (a) an 8-digit or 9-digit numeric code of the User’s choice; or (b) a 10-digit or 11-digit number corresponding to the User’s registered mobile number (including any future expansion of mobile numbers to 11 digits). In the event the user chooses a 10-digit number, the UPI Application Provider shall fetch the mobile number associated with the User and shall not permit manual entry of a 10-digit or 11-digit UPI Number by the User. The UPI Application Provider however shall ensure that the User shall have the ability, to link, de-link, deregister, or replace the UPI Number chosen by the User.

5.2 Payer PSP and UPI Application Provider shall route all mobile number-based transactions through the Numeric UPI ID Mapper only. Local resolution for mobile number-based transactions can only be initiated by the PSP and UPI Application Provider only where the response time from Numeric UPI ID Mapper is exceeding one (1) second. Any dispute, loss, liability arising from such local resolution shall be the responsibility of the respective Payer PSP and UPI Application Provider.

5.3 Payer PSP and UPI Application Provider shall ensure that when a User intends to initiate a UPI payment using Beneficiary’s UPI Number, the UPI Application used to make payment shall require the beneficiary's UPI Number to be entered twice and shall validate that both entries match before proceeding with the transaction. Notwithstanding the foregoing, if a User transfers funds to incorrect mobile number, the responsibility of the same shall lie with the User initiating the payment. This shall be made applicable to ensure that a wrong number is not entered by the User. The exception to the dual entry method can be:

(i) The User has saved the UPI Number as a beneficiary within the UPI Application used to make payment; or

(ii) The Beneficiary's UPI Number is selected from a contact saved on the User's device or within the UPI Application; or

(iii) Any such verified Users as deemed by PSP/ UPI Application Provider, however any wrong transfers disputes shall be resolved by such PSP/ UPI Application Provider.

5.4 Payer PSP and UPI Application Provider shall resolve the UPI Number and present the Beneficiary details to the User for verification and confirmation prior to processing any transaction initiated using a UPI Number.

5.5 The Numeric UPI ID Mapper shall rely exclusively on the latest successful mapping entry to identify the Payee PSP. For all UPI Number-based financial transactions, the Payer PSP and UPI Application Provider shall mandatorily pass the Payee UPI Number (Central Mapper Identifier (CMID)), together with all other applicable transaction fields, to facilitate accurate transaction processing and routing.

5.6 A User may maintain multiple UPI Numbers across different UPI Applications. However, where a mobile number is designated as a UPI Number, such mobile number shall be linked to only one UPI ID at any given time.

5.7 UPI Application Provider, including those offering feature phone-based and voice-based interfaces, shall enable UPI Number functionality and ensure lifecycle management, including creation/registration, update, and deletion or deregistration.

5.8 PSP and UPI Application Provider shall ensure that UPI Number is permitted only for Person-to-Person (P2P) transactions. PSP and UPI Application Provider are not permitted to allow PPI wallet Users to set-up a UPI Number.

5.9 Member Bank, PSP and UPI Application Provider shall utilize the Mobile Number Revocation List (MNRL)/ Digital Intelligence platform (DIP) and update their databases regularly. Further, UPI Application Provider and PSP are responsible for creating the User's profile in the UPI Application and issuing the corresponding UPI ID. The PSP and UPI Application Provider shall be liable for any omission, delay, or dispute/chargeback arising from the failure to update the Numeric UPI ID Mapper.

5.10 All PSP and UPI Application Provider shall, on an ongoing basis, monitor and identify UPI IDs and associated UPI Numbers, that have remained inactive, with no financial transactions, for a period exceeding one (1) year. Upon such identification, the concerned UPI IDs and UPI Numbers shall be disabled for inward credits, and the linked mobile numbers shall be deregistered from the Numeric UPI ID Mapper.

5.11 Payer PSP and UPI Application Provider shall ensure that a User shall be permitted to use the same UPI Number / UPI ID in situations such as SIM change or handset change if the same mobile number is used.

5.12 Payer PSP and UPI Application Provider shall ensure that any UPI Number, upon deregistration, shall not be allowed for re-registration/use for a period of 6 months for new Users. The existing User may reuse the UPI Number within this period.

5.13 Payer PSP and UPI Application Provider shall ensure that for a reassigned mobile number, usage of such mobile number shall be permitted only after 6 months from the last active transaction, or upon full onboarding, whichever is earlier.

5.14 User, for whom, inward credit transactions have been disabled on a UPI ID and associated UPI Number, or linked mobile number, the User shall mandatorily re-register on the UPI Application to re-establish Numeric UPI ID Mapper linkages and restore fund receipt capabilities. Restoration of inward credit functionality shall be contingent upon successful completion of the re-registration process. Users shall, however, continue to be permitted to perform outward financial and non-financial transactions using UPI PIN, biometric authentication for transaction, among others.

5.15 Payer PSP and UPI Application Provider shall obtain the User's explicit and informed consent before seeding or porting a UPI Number and shall provide a clear mechanism for opting out. The consent process shall be designed on an opt-in basis, requiring the User to actively provide consent, and shall not rely on pre-enabled or default selections or form part of the any form of terms and conditions. The Numeric UPI ID Mapper Consent Terms & Conditions will be periodically updated to incorporate new features, enhancements, and ecosystem initiatives such as UPI Circle.

5.16 Payer PSP and UPI Application Provider shall communicate UPI Number-related information to User in a fair, transparent, and unbiased manner. They shall not use misleading design elements, coercive prompts, pop-up blockers or undue influence to obtain User consent.

5.17 User's consent for the porting of a UPI Number shall be obtained through a separate and independent process in the User's profile section only. Any form of solicitation for such porting shall be prohibited. However, where a User has not been seeded (including first time registration) or has deregistered on UPI Number, UPI Application Provider shall notify the User to create a UPI Number. Payer PSP and UPI Application Provider may engage with Users through a balanced approach, provided that such engagement does not disrupt transaction flows and that appropriate User consent has been obtained.

5.18 If a User declines consent for seeding their details into the Numeric UPI ID Mapper, the User will not be able to receive funds using their UPI Number from any User, irrespective of whether the transaction originates from the same or a different Payer PSP or UPI Application Provider. However, the User shall continue to receive funds through their UPI ID or other payment addresses, such as their bank account number, QR code, among others

5.19 Payer PSP/ UPI Application Provider shall ensure the display of the beneficiary's name before processing a 'pay to contact', 'pay to mobile number', or any other transaction initiated using a mobile number. The beneficiary's name shall be displayed only as retrieved in real time, and no reliance shall be placed on locally stored or cached data for such display.

5.20 Payer PSP / UPI Application Provider shall ensure that all UPI System Requirements are applicable to UPI IDs including interoperability, mandatory home page display, and masking rules apply equally to

UPI Number. Additionally, all feature phone and voice-based UPI solutions shall adhere to the interoperability standards of UPI Number.

5.21 For feature phone and voice-based payment transactions, Payer PSP / UPI Application Provider shall authenticate transactions through the Server-Side Common Library (SSCL).

6. Types of UPI transactions

UPI transactions are classified into the following categories:

Sr. No.	Category	Description
1	P2P	Person to Person
2	P2M	Person to Merchant
3	P2PM	Person to Person Merchant
4	M2P/ B2C	Merchant to Person/ Business to Customer
5	M2M/B2B	Merchant to Merchant/ Business to Business

7. Merchant Onboarding, Classification and Transaction

Merchant transactions on UPI include Person-to-Merchant (P2M), Person-to-Person Merchant (P2PM) and Merchant-to-Merchant or Business-to-Business (M2M/ B2B) payment flows.

7.1 Payee PSP shall onboard Merchants on UPI as per their board-approved Merchant acquisition policy, which shall, at a minimum address acceptable Merchant types and Merchant Category Code (MCC) allocation criteria, merchant underwriting and due diligence, merchant agreements, portfolio and transaction monitoring, merchant training, and third-party agent risk oversight.

7.2 Small Merchants with an expected inward UPI transaction of less than or equal to ₹1 lakh shall be categorised under the P2PM category. MCC 7407 has been assigned for the P2PM category of Merchant and Payee PSP shall populate the correct MCC corresponding to the Merchant's actual business category in the 'subCode' field of the merchant tag in UPI to identify the nature of the Merchant's business. For P2PM transactions, the settlement of funds shall credit in real time to end Merchant's own account.

7.3 Payee PSP shall adhere to all MCC-wise requirements, including permitted transaction types, initiation modes and purpose codes, applicable limits and responsible entity obligations.

7.4 The responsibility and liability related to UPI merchant shall rest with the Payee PSP including, but not limited to, the accurate passing of Merchant genre, onboarding type, merchant type and other applicable merchant attributes.

7.5 The Payee PSP shall ensure that no surcharge is levied to Users for UPI transactions. In cases where any convenience fees are charged, the Payee PSP shall ensure that such fees are disclosed upfront to the User on the merchant payment page(s) prior to the selection of the payment mode. The Payee

PSP shall further ensure that such convenience fees remain consistent across the available debit payment modes (including net banking, debit card, UPI and credit card).

7.6 Payee PSP shall ensure that all application-based and mobile-web-based merchants enable Intent-based UPI payments, while all other web-based merchants enable dynamic QR code-based UPI payments.

7.7 The “Pay by any UPI Application” functionality shall be mandatory for all Merchant payment journeys, including online application-based and web-based merchant flows. Payee PSP shall ensure that both directly and indirectly acquired Merchants accept UPI payments from all UPI Application Provider, without any restriction, with appropriate UPI branding and visibility to Users. Acceptance of UPI payments through selective group or specific UPI Application Provider shall not be permitted, in line with the principle of UPI interoperability.

7.8 A large Merchant, whether online or offline, may be classified as a Verified Merchant by the Payee PSP upon completion of due diligence if it belongs to the capital markets, insurance, government e-marketplace, credit card bill payments, collections, foreign exchange retail through Bharat Bill Pay System (BBPS), tax payment, Initial Public Offering (IPO), Reserve Bank of India (RBI) G-Sec or government merchant segments, or has a consolidated annual turnover, including that of its group entities, of at least ₹50 crore in the preceding financial year. The Payee PSP may prescribe additional conditions under its Board-approved policy and shall maintain and regularly update the Verified Merchant list, remove Merchants that no longer meet the prescribed criteria. UPI Application shall display the Verified Merchant indicator (Green Tick) and communicate the availability of enhanced transaction limits to Users, wherever applicable.

7.9 Payee PSP shall not allow intent-based transactions for offline non-verified merchants. Additionally, Payer PSP shall ensure that P2P intent-based transactions are not allowed.

8. UPI Plug-in

UPI Plug-in enables a PSP to extend its PSP Software Development Kit (SDK) (Parent Application) for integration with a Merchant application (Partner Application). The Partner Application shall provide Users with an inline payment experience through the Parent Application SDK.

8.1 The Partner Application shall provide UPI merchant functionalities in accordance with the partner’s Merchant payment needs as per their business use case.

8.2 The Partner Application shall operate as a non-exclusive PSP handle (where the handle is common across multiple applications), where the Partner Application will have the same profile (UPI ID and remitter account of the User) already present in a PSP application which manages UPI IDs.

9. Biometric Authentication

9.1 Biometric Authentication enables Users to securely authenticate UPI transactions using biometrics (including fingerprints, facial recognition, and other supported biometric methods) already registered on their devices, as an additional option in place of, or as an alternative to, UPI PIN.

9.2 Payer PSP/ UPI Application Provider shall validate device compatibility and security validations before authentication. These validations shall include but not be limited to, checks for rooted or jailbroken devices, unsupported operating system versions, device compatibility, and validating biometric enrolment, before authentication.

9.3 Remitter Bank shall check User eligibility (as per bank's policy) and validate authentication credentials, before authorizing the transaction. (Including UPI PIN, biometric enablement, among others).

9.4 Payer PSP/ UPI Application Providers shall obtain the User's explicit and informed consent for enabling biometric authentication. Fresh consent shall be required after every device binding and any addition or re-enrolment of biometric credentials (fingerprint, face, among others) on the device, with the User having ability to opt out at any time.

9.5 Remitter Bank shall notify Users (through SMS, email or any other appropriate communication channels) upon successful enablement / disablement of biometric authentication.

9.6 Remitter Bank shall disable the biometric authentication method for the User's account for all UPI Application Providers in case of a UPI PIN change or reset. Remitter Bank shall ensure to decline subsequent transaction using biometric authentication with appropriate response code until the User re-enables the biometric authentication and provides fresh consent.

9.7 Payer PSP/ UPI Application Providers shall ensure that key rotation operation is undertaken within one year from the date of biometric enablement.

9.8 UPI Application Provider shall make biometric authentication inactive, if the User has not performed any transaction by this method within 90 days and shall be activated only upon User confirmation with UPI PIN.

10. User Support and UPI Safety Awareness

Members and UPI system participants shall ensure that Users are duly notified of all UPI-related activities via their registered channel, as per the extant regulatory guidelines.

10.1 UPI Application Provider shall educate Users on safe UPI usage through multilingual awareness content during onboarding and prominently display a 'How to Use UPI Safely' awareness video during first-time installation and initial launch. Where in-app playback is not supported, a link to the video shall be provided. The video shall support multiple language options.

10.2 Remitter Bank shall enable Users to block or disable UPI services upon request through designated support channels.

10.3 Members and PPIs shall provide timely notifications for all UPI debit, credit, reversal and post-reconciliation account entries.

11. Data Privacy, Data Protection and Customer Information Management

Member, Sub-Member and UPI Application Provider shall ensure that the processing, including collection, access, use, storage, transmission, sharing and disposal, of any personal data or payment-related information, including any User information, is undertaken in a secure, lawful and accountable manner, in compliance with

Applicable Laws. Further Member, Sub-Member and UPI Application Provider shall implement applicable, required governance and compliance frameworks, including no less restrictive than industry standard controls and measures, for such processing.

12. UPI API Usage

The use of the UPI APIs by the Members shall follow the usage norms as per UPI System Requirements and strictly for the purpose of processing financial or non-financial transactions initiated by the User, risk management and fraud prevention or otherwise as specified by NPCI. APIs, especially standalone APIs, may not be used other than for their intended purpose. Members to route all financial and non-financial UPI transactions (including on-us) through NPCI.

12.1 With the objective of streamlining the performance of UPI, the response time for UPI APIs initiated by NPCI is as follows:

Sr. No.	UPI API	Entities	Response Time
1	Request Pay, Response Pay (Debit and Credit)	Remitter Bank; Beneficiary Bank	15 seconds
2	Check Transaction Status	Remitter Bank; Beneficiary Bank	10 seconds
3	Transaction Reversal (Debit and Credit)	Remitter Bank; Beneficiary Bank	10 seconds
4	Validate Address (Pay, Collect)	Payer PSP; Payee PSP; Beneficiary Bank (Account and IFSC based transactions)	10 seconds

12.2 PSP shall ensure that all the API requests (traffic) sent to UPI are monitored and moderated in terms of appropriate usage — e.g. restricting a high number of repeat APIs for the same transaction or older transactions, among others.

12.3 PSP shall ensure that there is no batch processing (by processing a file and converting it to an online request at high Transaction Per Second (TPS) limitations) of any of the financial/non-financial APIs sent to UPI system.

12.4 PSP shall initiate check transaction status APIs as guided in section UPI API Usage Guidelines. Subsequently, in case of U48 error (Transaction ID not present or not found in UPI System) within the first two hours from initiation of the original transaction, PSP shall refer to the NPCI settlement files after the settlement cycle is completed; alternatively, Members may initiate a maximum of one check transaction status API on Unified Dispute and Issue Resolution (UDIR), which in turn checks Unified

Real-time Clearing and Settlement (URCS) (UPI Backoffice) to fetch the final settlement status of the transaction.

12.5 PSP shall consider the transaction failed if they receive an error in check transaction from the list mentioned in Annexure C and shall not initiate a further check transaction status API.

12.6 The Remitter Bank/PSP shall ensure visibility over UPI APIs and is responsible for regularly reviewing their usage. Any exceptions or anomalies observed shall be reported to NPCI.

12.7 PSP shall ensure that all the API requests (in terms of velocity and TPS limitations) sent to UPI are monitored and moderated in terms of appropriate usage (User-initiated and PSP system-initiated).

12.8 With the objective of improving the performance of UPI, shall adhere to the following:

Sr. No.	API/Use cases	Purpose	Frequency / Limits	Usage Guidelines
1	Balance Enquiry	This API is used to check balance available through UPI Application Providers.	50 per application per User per day 24 hours rolling#)	a) These requests shall be initiated only by the User. b) UPI Application Providers shall have the capability to limit or stop balance enquiry requests, if needed to reduce the load in peak hours. c) Remitter Bank shall add the available balance with every successful UPI financial transaction communication. d) The User account balances cannot be stored or used by Payer PSP or UPI Application Providers.
2	List Keys (for type ListKeys and PSPKeys)	This API allows the PSPs to request the list of public keys at NPCI.	Only once per PSP per day (24 hours rolling)	a) Minimum page size of 1000 to be used while initiating the request. b) To be done in non-peak hours.

Sr. No.	API/Use cases	Purpose	Frequency / Limits	Usage Guidelines
3	List Account	This API allows a User to find the list of accounts linked to their mobile by a particular account provider.	25 per application per User per day (24 hours rolling)	a) These requests are to be initiated only once the User selects the Remitter Bank in the UPI Application. b) In case of failure to list account, every re-try shall be done only with User consent.
4	Check Transaction Status	This API allows the PSPs to request for the status of the transaction.	Maximum of 3 check transaction status APIs, preferably within 2 hours from the initiation/authentication of the original transaction.	The PSPs shall request for status only after 60 seconds of the initiation/ authentication of the original transaction.
5	AutoPay Mandate Execution	Executing UPI AutoPay mandates.	Maximum of 1 attempt and 3 retries per mandate (per sequence number) shall be permitted.	a) Initiator PSPs to ensure UPI AutoPay executions are initiated at moderated TPS. b) To be initiated in non-peak hours.
6	List Verified Merchants	This API is used by the PSPs to manage and access the verified address entries (Verified Merchants).	Once per PSP per day (24 hours rolling)	a) Minimum page size of 1000 to be used while initiating the request. b) To be done in non-peak hours.
7	Penny Drop	Transactions initiated to verify the validity	Queueing shall be maintained at initiating PSP end.	a) This shall be extended only to entities where it is a regulatory requirement.

Sr. No.	API/Use cases	Purpose	Frequency / Limits	Usage Guidelines
		and ownership of an account.		b) This shall be initiated only with explicit User consent (the initiating bank shall have a formal undertaking from the requestor and be in full compliance with the Digital Personal Data Protection Act (DPDP) Act, 2023 and revised time to time. c) MCC 7413 and a separate dedicated UPI ID shall be assigned by the entity for such transactions. d) To be initiated in non-peak hours.
8	ValCust API	This API is used to validate the User details, pre-debit notification, User activation for FIR, among others	Service shall be allowed to be used only for valid use cases.	a) For IPO, PAN validation shall only be initiated where the mandate has been successfully created. b) For other use cases it shall be initiated in limited attempts and at moderate TPS.
9	API Header Format	PSPs to ensure that only the mentioned headers shall be leveraged in UPI API traffic.	Permitted headers: a) Host; b) Content-Length; c) Content-Type/Accept; d) User-Agent.	a) All Members shall update their production API clients and reverse proxies to whitelist only the permitted headers. b) Preventive mechanisms shall be configured at the appropriate level (e.g.

Sr. No.	API/Use cases	Purpose	Frequency / Limits	Usage Guidelines
				reverse proxies, API gateways) to reject or strip out unauthorized headers.
10	Validate Address*	This API is used for validating UPI IDs or Virtual Payment Addresses (VPAs) before initiating a payment or transaction.	NA (NPCI may release updated limits later).	a) To be used only when the User intends to pay. b) Stand-alone use of Validate Address is not permitted. c) Where Validate Address is used for the penny drop use case, the MCC (7413) defined for penny drop shall be used for Validate Address as well. d) Appropriate credentials of the initiator (mobile number, UPI ID, MCC, etc.) shall be populated in payer details API fields.

** NPCI may deploy rate limiters for this API.*

 # Rolling period refers to time calculated from the time of first successful request

12.9 In addition to the above, Members are to note the following:

12.9.1 PSP shall monitor and maintain queueing of system-initiated APIs to ensure moderated TPS — in other words, PSP systems shall not be a pass-through for back-end generated API transactions to UPI systems in any condition.

12.9.2 During peak hours, Members are required to restrict non-User-initiated APIs.

12.9.3 PSP and PPI Issuers shall audit their systems by a CERT-In empanelled auditor to review the API usage and existing systems behaviour annually by May 31, for previous financial year. For the audit scope, PSPs shall refer to UPI Procedural Guidelines.

12.9.4 The User data (PII Data – Personally Identifiable Information) to reside in bank or bank owned data center and the same shall not be passed to any party including that of Merchant or Intermediary unless specified by the industry regulator as the regulatory requirement or otherwise approved by NPCI specifically.

12.9.5 Members shall refer to the UPI System Requirement for details on UPI API usage and monitoring.

13. UPI Branding

13.1 Member and UPI Applications Providers shall comply with the applicable BHIM UPI brand guidelines and other UPI brand requirements prescribed by NPCI from time to time, including but not limited to requirements relating to UPI logo/mark usage, “Powered by UPI” display, UPI ID visibility, customer-facing UPI payment screens, User awareness content, among others.

13.2 Payee PSP shall ensure that all new Merchant QR codes issued, and all existing Merchant QR codes being replaced, on or after December 1, 2026, shall mandatorily be compliant with the updated BHIM UPI Merchant QR Brand Guidelines.

13.3 Payee PSP shall obtain approval for all Merchant QR code from NPCI before implementation.

Part III – UPI FEATURES AND SERVICES

14. UPI AutoPay

UPI AutoPay is a Mandate registered by a User on UPI to enable automated debits for pre-agreed recurring payment requirements across various categories, including subscriptions, bill payments, insurance, financial services, loan repayments, auto-replenishment of NETC FASTag and RuPay National Common Mobility Card (NCMC), among others. Members shall read the UPI AutoPay rules and regulations applicable in UPI in conjunction with extant Applicable Laws.

14.1 UPI Application Provider and Payee PSP shall mandatorily enable the Intent and QR flow for UPI AutoPay Mandate registration.

14.2 Payee PSP and UPI Application Provider shall ensure that the first debit amount is displayed separately for mandates registered through QR and Intent modes.

14.3 Remitter Bank and Payer PSP/ UPI Application Provider shall send SMS and communication/ notification respectively to the User for every UPI AutoPay transaction including mandate registration, pre-debit notification, execution, post-debit notification, modification, pause, unpause and revoke transactions.

14.4 Member shall ensure that the User completes a one-time registration process and that a mandate is registered only after successful validation of Additional Factor of Authentication (AFA), in addition to the normal process required by the Remitter Bank.

14.5 Every Mandate registered on UPI shall specify the validity period of the Mandate. Payee PSP shall ensure that the maximum validity period does not exceed 30 years. Payee PSP through Merchant shall ensure that the Users are provided with an option to edit the Mandate validity period/ end date at the time of registration.

14.6 Member shall ensure that the Mandate may be registered for either a pre-specified fixed amount or for a variable amount. In the case of variable amount mandates, the Remitter Bank shall provide the User with a facility to specify the maximum value of any recurring transaction.

14.7 Remitter Bank shall ensure that the User shall be given a facility to choose or change a mode among available options (SMS, email, etc.) for receiving the pre-debit notification.

14.8 Remitter Bank and Payer PSP/ UPI Application Provider shall send a pre-debit notification to the User at least 24 hours prior to the actual charge/ debit which shall at the minimum, inform the User about the Merchant's name, transaction amount, date and time of debit, UMN (Unique Mandate Number), reason for debit.

14.9 Payee PSP shall ensure that pre-debit notification transaction is initiated at least 24 hours prior to the actual charge/ debit.

14.10 Member shall ensure that Mandate registered to auto-replenish balances of FASTag, UPI LITE auto top up and National Common Mobility Card (NCMC) are exempt from pre-debit notification requirements.

14.11 Remitter Bank and Payer PSP/ UPI Application Provider shall ensure that the first transaction in UPI AutoPay is with AFA validation. If the first transaction is executed along with mandate registration (within 5 minutes of registration), the AFA for mandate registration and the first transaction may be combined, provided the transaction amount is up to ₹15,000 or ₹1,00,000 per transaction, as per applicable MCC.

14.12 Remitter Bank and Payer PSP/ UPI Application Provider shall ensure that subsequent recurring transactions below ₹15,000 or ₹1,00,000 per transaction as per applicable MCC does not require Additional Factor of Authentication (AFA) from the User. Transactions beyond the defined limit shall require AFA.

14.13 During Mandate execution, Remitter Bank shall validate the Digital Signature Certificate (DSC) and AFA for execution amount more than ₹15,000 or ₹1,00,000 per transaction as per applicable MCC and for execution amount below the threshold shall process the execution basis the DSC only.

14.14 Payments under UPI AutoPay shall not be subject to any other limits / controls set by the User.

14.15 Remitter Bank shall send a post-debit notification to the User which shall at the minimum, inform the User about the Merchant's name, transaction amount, date and time of debit, Unique Mandate Number (UMN), reason for debit and details on grievance redressal.

14.16 Remitter Bank shall provide the User with a facility to modify the validity period of the Mandate at any point of time. Information about this facility shall be clearly communicated to the User at the time of registration.

14.17 Payee PSP shall ensure that Merchants provide the User with a facility to modify amount.

14.18 Remitter Bank shall provide the User with a facility to opt-out of any particular transaction (pause) or revoke the mandate.

14.19 Payer PSP/ UPI Application Provider shall provide Users with a facility to revoke or pause Mandates except for the Loan Payments and EMI Collection categories.

14.20 Payee PSP shall ensure that Merchants accepting payments through UPI AutoPay shall support the Mandate pause functionality.

14.21 For all Merchant segments, the Payee PSP shall ensure that a provision to revoke the Mandate is made available to the User on Merchant's website or application. For such requests, Payee PSP shall send the revocation request to the UPI AutoPay channel instead of deleting the Mandate only on the Merchant end.

14.22 For any Mandate operation, where the request fails due to Mandate having been revoked or not existing, Members shall remove that corresponding Mandate at their end as well.

14.23 UPI AutoPay Mandate withdrawal through Merchant platform does not require AFA validation for UPI.

14.24 Mandate interoperability

14.24.1 Payer PSP and UPI Application Provider shall ensure complete lifecycle management, including viewing and porting of a User's UPI AutoPay Mandate on the respective application, under the 'Manage Bank accounts' or the dedicated 'UPI Autopay' section.

14.24.2 Payer PSP and their UPI Application Provider shall not store or utilize Mandate details obtained through the 'View Mandate' function for any other purpose.

14.24.3 UPI Application Provider shall ensure that the 'Port Mandate' option is strictly User-driven only, accessible from the Mandate details page fetched with 'View Mandate'. No inducements, including cashback, incentives, notifications, banners, nudges, alerts, or any app-based/non-app-based implementation, shall be employed to solicit Mandate portability.

14.24.4 'Port Mandate' can be done thrice in a rolling 90-day period.

14.24.5 Payee PSP shall generate a unique Merchant Identifier Code (MIC) mandatorily for every Merchant in a standardized manner. Merchant can choose to execute UPI AutoPay Mandates through any Payee PSP, provided the appropriate MIC and other Mandate details are passed.

14.24.6 Member shall ensure that the Merchants shall be able to update their existing UPI ID without alteration of the MIC and other Mandate parameters.

14.24.7 Payee PSP shall ensure that the payee UPI ID updation for an active UPI AutoPay Mandate is allowed only in scenarios arising out of regulatory direction or discontinuation of services by the Payee PSP.

15. UPI One Time Mandate (OTM)

UPI OTM enables Users to pre-authorise transactions by blocking funds in their account at the time of Mandate registration, with the actual debit happening upon transaction execution.

15.1 Members shall ensure that the Mandate are registered through QR, Intent, collect, among others and shall not be initiated by the Payee PSP for P2P transactions.

15.2 Members shall ensure that the User undertakes a one-time registration process and that the Mandate is registered only after successful validation of Additional Factor of Authentication (AFA).

15.3 Remitter Bank shall post successful response only after blocking the requisite funds in the User's account and shall bear liability if such funds do not remain blocked thereafter.

15.4 Remitter Bank and Payer PSP shall validate the digital signature and verify the parameters during Mandate execution or debit processing.

15.5 Members shall ensure that a Mandate is executed only up to the amount authorized by the User. Once executed and if partial, Remitter Bank shall unblock the remaining amount in the User's account. Remitter Bank shall unblock the amount after expiry of the Mandate.

15.6 In case of revocation initiated by Payee PSP, the block on the money shall be released immediately and the money shall be reinstated to the User's account by the Remitter Bank. Payee PSP shall ensure that the execution date precedes the revocation date or expiry date.

15.7 Post-debit SMS and communication/ notification to the User shall mandatorily be sent for create, update, revoke and debit by Remitter Bank and Payer PSP/ UPI Application Provider respectively.

15.8 Member shall support UPI-based User validation using PAN for use cases permitted by NPCI (UPI OTM for Application Supported by Blocked Amount (ASBA) based Initial Public Offering (IPO) process).

15.9 Member shall ensure that for Bima Application Supported by Blocked Amount (Bima-ASBA) facility, the block period shall not exceed fourteen (14) days from the date of registration or the completion of underwriting, whichever is earlier.

16. UPI Reserve Pay

UPI Reserve Pay (formerly referred to as Single Block Multiple Debits (SBMD)), is a Mandate facility under which a User authorises a block of funds in its bank account, against which a Merchant may initiate multiple successive debits until the blocked amount is fully exhausted or the Mandate expires, or it is revoked.

16.1 Member shall ensure that UPI Reserve Pay supports all account types permitted under UPI (including Savings Account (SA), Current Account (CA), Overdraft (OD), RuPay Credit Cards, pre-sanctioned Credit lines, among others) for Merchant segments.

16.2 Member shall ensure that UPI Reserve Pay Mandates are applicable only for P2M transactions.

16.3 Remitter Bank shall support UPI Reserve Pay by having a mechanism to create blocking of funds in the User's account and shall allow multiple debits against the block wherein the fund shall remain blocked in the account till the time mandate is expired, revoked or the mandate amount is exhausted.

16.4 Remitter Bank shall ensure that a User, identified through a unique mobile number, is permitted to create only one active block at a time for a particular Merchant.

16.5 UPI Application Provider shall support UPI Reserve Pay functionality and provide an interface for the User to process the transactions.

16.6 Payee PSP shall ensure that the block created shall not be treated as the guarantee of payment, only the successful debit response received by the Merchant (for the debit initiated by the User action on Merchant's platform) shall be considered for payment.

16.7 Payee PSP shall ensure that the purchase action by the User shall result into instant debit request without any delay, and the delivery of goods and service shall only be after the confirmation of successful debit for categories such as quick commerce, food delivery, among others. For use cases wherein amount is not fixed and is determined based on the services consumed (e.g.: cab aggregators, EVs, among others), Merchant may debit post successful delivery of services.

16.8 Member shall ensure that the current block limits (unutilized) are always checked before initiating a debit.

16.9 Payee PSP shall ensure that Merchant provides the User with facility to modify amount or validity period.

16.10 Payee PSP and UPI Application Provider shall ensure to provide the User with a facility to revoke UPI Reserve Pay Mandates.

16.11 Remitter Bank and Payer PSP/ UPI Application Provider shall notify the User in the form of SMS and Communication/ notifications respectively for all Mandate operations i.e. block creation, modification, debit, revoke and expiry.

17. UPI Circle

UPI Circle enables a Primary User to authorize a trusted Secondary User and Internet of Things (IoT) device to perform UPI transactions on the Primary User's behalf, without requiring the Primary User or the Primary User's device to be physically present at the point of transaction.

This feature provides the Primary User with visibility and control over transactions undertaken by the Secondary User and IoT device, in accordance with the applicable security protocols and transaction limits. UPI Circle is intended to facilitate delegated payment use cases, reduce reliance on cash, and promote financial inclusion for trusted Users including minors, spouses, and connected devices.

UPI Circle supports the following types of delegation:

(i) Full Delegation: The Primary User authorizes a Secondary User and IoT device to initiate and complete UPI transactions within the limits set by the Primary User. Delegation to IoT devices shall be supported only under Full Delegation.

(ii) Partial Delegation: The Secondary User may initiate a UPI transaction, which shall be completed only upon authorization of each payment request by the Primary User.

17.1 Payer PSP/ UPI Application Provider shall offer independent User journeys for Primary and Secondary User/ Things (IoT) device. UPI Application Provider and PSP shall ensure interoperability across linking and transaction journeys.

17.2 During the linking of a Secondary User under Full Delegation, Payer PSP of Primary User shall share the additional details (document type and document ID number) of the Secondary User to the Payer PSP of Secondary User and Remitter Bank. The Remitter Bank shall identify the Secondary User based on User's name, mobile number and identification number of an officially valid document as defined in the existing regulatory guidelines on KYC.

17.3 During the linking process of Full Delegation, Payer PSP of Secondary User shall obtain the explicit consent from Secondary User on additional details shared before linking request acceptance.

17.4 Payer PSP of Secondary User shall capture device/ User identifiers details from Secondary device during registration and shall validate during payment request. Remitter Bank shall validate device/ User identifiers and requisite authorization details for every transaction before debiting the account for payment.

17.5 Secondary Payer PSP/ UPI Application Provider shall ensure that same mobile number is used for IoT and UPI Circle registration.

17.6 Linking and other lifecycle management actions shall be authenticated using Additional Factor of Authentication (AFA) for Full Delegation and can be completed through the User's respective UPI Application.

18. UPI LITE

UPI LITE is designed to process low value transactions without Additional Factor of Authentication (AFA) by maintaining an on-device wallet. UPI LITE reduces load on core banking systems in real-time. Once UPI LITE is enabled, the User shall be able to allocate funds from its bank account to UPI LITE.

UPI LITEX is an extension of UPI LITE and is designed to enable offline, proximity-based payments through Near Field Communication (NFC), allowing Users to complete transactions without internet connectivity. The solution operates through LITE balances on devices, ensuring instant payments without reliance on network connectivity.

Above-mentioned funds shall reside with the Remitter Bank in a designated account and mirror copy of the same shall reside on User's device in the Common Library (CL) of the relevant UPI Application. The Remitter Bank shall debit the User's bank account and manage the UPI LITE funds on receipt of UPI LITE top-up requests.

18.1 For new User onboarding, UPI Application Provider shall enable UPI LITE as part of the UPI onboarding process with requisite consent from the User and shall make UPI LITE mandatory for less than ₹500 value transaction. This shall be applicable for UPI Application where no account types other than Current Account(s) or Saving Account(s) (CASA) are linked.

18.2 Payer PSP/ UPI Application Provider, and Remitter Bank shall ensure that User is able to enable, disable and top-up (User-initiated/Auto Top-up) the UPI LITE at any point in time and the fund transfer between the UPI LITE and User's bank account shall be processed in real-time.

18.3 Payer PSP/ UPI Application Provider and Remitter Bank shall implement 'Transfer Out' functionality which allows Users to withdraw funds from their UPI LITE balance to source bank account from which such funds were loaded, without disabling UPI LITE.

18.4 UPI LITE enablement and top-ups shall be completed only upon successful AFA validation by the Remitter Bank.

18.5 UPI Application Provider shall display all relevant UPI LITE information to the User, including UPI LITE balance, transaction status and top-up details, among others. UPI LITE transactions shall be clearly distinguished from regular UPI transactions in the transaction history, and the UPI LITE balance shall be prominently displayed on the home screen of the UPI Application.

18.6 Payer PSP/ UPI Application Provider shall ensure that UPI LITE services are not offered on rooted or jailbroken devices (unsecured) mobile phones.

18.7 UPI Application Provider shall provide Users with the option to top up their UPI LITE balance through either of the following methods:

(i) User-initiated top-up: by authorizing the top-up with AFA.

(ii) LITE Auto top-up: enabled by User with AFA to set up automatic replenishment of the UPI LITE balance from a linked bank account.

18.8 UPI Application Provider/ Payer PSP shall ensure that User is provided with the options to enable UPI LITE Auto Top-up and Remitter Bank shall support the enablement and processing of such Auto Top-up transactions.

18.9 UPI LITE Auto Top-up transaction is exempted from Pre-Debit Notifications (PDNs) sent by the Remitter Bank and UPI Application Provider/ Payer PSP.

18.10 Remitter Bank shall identify all the UPI LITE accounts that have no transactions during the preceding six (6) months. Any balance remaining in such dormant UPI LITE accounts shall be refunded to the respective source bank account and the corresponding LITE Reference Number (LRN) shall be deleted.

18.11 Remitter Bank shall be responsible for maintaining LRN-wise transaction information/balances and ensuring reconciliation of such information/balances with their internal records and settlement data. Remitter Bank shall ensure that adequate systems, controls, and monitoring mechanisms are in place for accurate LRN-wise tracking and reconciliation.

18.12 Remitter Bank shall ensure that UPI LITE balance is non-interest bearing.

18.13 Payer PSP/ UPI Application Provider shall ensure that only one UPI LITE account is permitted per UPI Application.

18.14 UPI Application Provider shall obtain the User's explicit consent prior to enabling UPI LITEX payments

18.15 Members shall adhere to UPI LITEX Brand Guidelines.

19. Conversational Payments (UPI 123Pay & Hello! UPI)

UPI 123Pay and Hello! UPI provide secure, accessible, and convenient payment solutions which can be accessed through feature phone or smartphone, thereby enabling financial inclusion and deepening digital payment adoption. UPI 123Pay enables UPI services through IVR-based payments, missed call-based payments and pre-installed application in feature phone.

Hello! UPI provides a conversational payment experience that enables Users to perform financial and non-financial UPI transactions through voice interactions. Users can initiate onboarding, balance enquiry, fund transfers, merchant payments and other UPI services using voice commands.

19.1 UPI 123Pay

19.1.1 Member shall enable Server-Side Common Library (SSCL) hosted at NPCI end for secure transaction authentication for feature phone and voice-based payments.

19.1.2 Member shall implement UPI Number in UPI 123Pay functionality through integration with UPI Numeric ID Mapper.

19.2 Hello! UPI

19.2.1 UPI Application Provider shall ensure that enablement and disablement of 'Hello! UPI' is through explicit consent of the User.

19.2.2 UPI Application Provider shall ensure voice-initiated transaction is authorized with AFA wherever applicable.

20. UPI Tap & Pay

UPI Tap & Pay is a contactless payment capability that enables Users to make UPI payments by tapping their NFC enabled mobile device. This provides a fast, secure, and frictionless contactless payment experience leveraging NFC technology, enhancing convenience for transactions. UPI Tap & Pay is inclusive (accessible to NFC-enabled device), multi-channel (proximity-based payment initiation), User-friendly (simply tap), and fully interoperable (across all PSPs).

20.1 Payer PSP/UPI Application Provider shall ensure to provide the UPI Tap & Pay mode of payment only on NFC-enabled mobile devices with explicit User consent.

20.2 UPI Application Provider shall provide a separate call to action button for UPI Tap & Pay.

20.3 Member shall ensure that limits for UPI Tap & Pay transactions through UPI LITE is as per current UPI LITE limits. Transaction amount greater than UPI LITE limit will require AFA.

21. Cash Deposit and Withdrawal through UPI

21.1 UPI Cash Withdrawal at Business Correspondent (UPI Cash Point)

UPI Cash Withdrawal at Business Correspondent (BC) touch points aims to extend interoperable cash withdrawal services through UPI at Micro ATM enabled Business Correspondent (BC).

It expands digital payment accessibility while enabling Users, particularly in semi-urban and rural regions, to access cash conveniently through local BC networks without dependency on debit cards, traditional ATMs or bank branches. Users shall be able to withdraw cash at authorised BC touch points by scanning a dynamic UPI QR code generated by the BC application and authenticating the transaction using the extant factor of authentication in UPI.

21.1.1 Payee PSP shall be responsible for onboarding of BCs as per the existing regulatory and legal framework issued from time to time. Transactions shall be initiated only through authorised BC touchpoints and BC applications.

21.1.2 Payee PSP shall ensure that such transaction is initiated through dynamic UPI QR codes generated at BC touch points. Payer PSP/ UPI Application Provider shall ensure the parameters present in the QR code is passed without any change.

21.1.3 UPI Application Provider shall not permit UPI Cash Point transactions through UPI LITE or any similar mode as each transaction must mandatorily require AFA. UPI Application Provider, PSP, or Remitter Bank shall not transactions through Credit accounts for UPI Cash Point.

21.2 Cash withdrawal at Merchant location using UPI (Cash at Point-of-Sale, PoS)

Users can withdraw cash at merchant location using UPI similar to the existing facility available Cash at Point-of-Sale (PoS) enabled by cards.

21.2.1 Payee PSP, UPI Application Provider, and Remitter Bank shall, in accordance with their respective roles, undertake the applicable due diligence and ensure compliance with all relevant requirements, including, but not limited to, merchant onboarding, limit management, and the processing of transactions in accordance with the prescribed parameters and controls.

21.2.2 Payee PSP shall ensure that the facility is available irrespective of whether the User makes a purchase or not.

21.2.3 Payee PSP shall ensure provision of a User service grievance redressal mechanism including issues related to disbursement of counterfeit currency by the on-boarded merchants. It shall also ensure compliance to the instructions stipulated by extant regulatory guidelines in respect of KYC and AML.

21.3 Cash Withdrawal at ATM using UPI (UPI ATM)

Interoperable Card-less Cash Withdrawal (ICCW) is a service which allows a User to withdraw the cash at any ATM terminal using UPI (without using debit card). This service can be availed at ATMs including White Label ATM without using their card.

21.3.1 Members shall mandatorily implement ICCW online reversals. ICCW reversals are further categorised into two types as ‘ATM-induced reversals’ and ‘Auto reversals’ to be used for failed transactions as mentioned below:

(i) ATM Induced reversal – This is when debit is successful in UPI, transaction reaches NFS, but ATM cash dispense fails.

(ii) Auto Reversal – This is when debit occurs in UPI, but the transaction further does not reach NFS, or post UPI debit no further requests is generated to complete the transaction.

21.3.2 Payee PSP shall ensure that only ICCW transactions are allowed to process on their ATMs. Additionally, they shall implement switch-level validations for Payee ATM VPAs to verify the above tags combination. Any transaction that does not meet the required combination must be declined by Payee PSP.

21.4 Cash Deposit using UPI (UPI ICD)

Interoperable Cash Deposit (UPI-ICD) is a cardless cash deposit service that enables Users of Member Banks to deposit cash at any UPI-enabled Cash Deposit Machine (CDM) or Cash Recycler Machine (CRM) deployed by banks or White Label ATM Operators (WLAOs), using UPI instead of a physical debit card. The deposits can either be self-deposit or third-party deposits meaning either in own account or non-own account.

21.4.1 Member Banks shall ensure that correct MCC, initiation modes and purpose codes are allowed for this transaction.

21.4.2 Payee PSP shall have a validation to decline any other non CDM transaction coming with other than defined initiation mode, purpose code and respective MCC.

21.4.3 Payee PSP to send notification to CDM through QR server / middleware/ ATM Acquirer Switch once the UPI transaction is successful.

21.4.4 Upon successful validation of beneficiary, Payee PSP to send the details (name and account number) of beneficiary to display on the CDM screen for depositor/User.

22. UPI Multi-Signatory

UPI Multi-Signatory feature enables UPI transactions that require authorization from multiple signatories. Transaction initiation, approval and execution shall be carried out in accordance with the authorization matrix defined and maintained by the Remitter Bank depending on the nature and hierarchy while operating the account.

22.1 Remitter Bank shall enable and manage UPI multi-signatory accounts, including signatory management and transaction authorization in accordance with account operating instructions.

22.2 UPI Application Providers shall provide the necessary interface to facilitate UPI multi-signatory accounts, including onboarding, transaction authorization, signatory information, transaction history, and life cycle management.

22.3 Remitter Banks shall enable current accounts, savings accounts and overdraft accounts for UPI Multi-Signatory functionality.

23. UPI International

UPI International enables the extension of UPI services beyond the geographical boundaries of India, facilitating cross-border payments. This supports interoperable payment capabilities for Indian Users to transact internationally, as well as for foreign Users to transact within India using UPI.

23.1 UPI Global Acceptance

UPI Global Acceptance enables Indian Users to make UPI transactions at international merchant locations using UPI. It supports interoperable QR-based payments, including UPI QR, proprietary QR and ISO-based QR, with NPCI facilitating transaction processing, routing, and translation into the UPI ecosystem. It is designed to provide a seamless and scalable payment experience for Indian Users travelling abroad while ensuring compatibility across multiple international geographies and payment infrastructures.

23.1.1 Payer PSP/UPI Application Provider and Remitter Bank shall obtain explicit User consent prior to enabling or processing UPI global acceptance transactions

23.1.2 Payer PSP/UPI Application Provider and Remitter Bank shall enable UPI Global Acceptance and support the addition of new countries through configurable changes. The latest list of enabled country codes and currency codes is provided in Annexure B.

23.1.3 Payer PSP/ UPI Application Provider shall ensure that QR Share & Pay (static sharing of QR images) shall not be permitted for UPI Global Acceptance transactions.

23.2 UPI Reverse Acceptance

UPI Reverse Acceptance enables international Users, travelling to India, to make Person-to-Merchant (P2M) payments to Merchants in India using their international mobile payment applications by scanning UPI QR codes.

23.2.1 Payee PSPs shall ensure that merchants UPI QR codes are enabled to accept transactions initiated through international mobile payment application.

23.2.2 Payee PSP and Beneficiary Bank shall enable UPI Reverse Acceptance and support the addition of new countries through configurable changes. The latest list of enabled country codes and currency codes is provided in the Annexure B.

23.3 Foreign Inward & Outward Remittances (FIR & FOR)

This enables Users to receive Foreign Inward Remittances (FIR) and initiate Foreign Outward Remittances (FOR) through UPI, facilitating cross-border peer-to-peer (P2P) transactions.

23.3.1 Payee PSP and Beneficiary Bank shall support interoperability for processing of FIR transactions.

23.3.2 Payee PSP/UPI Application Provider shall obtain explicit User consent prior to enabling or processing FIR transactions.

23.4 Domestic Processing of Foreign Inward Remittance

Domestic processing of Foreign Inward Remittance (FIR) through UPI enables credit of funds received from abroad into Beneficiary Bank accounts in India through UPI domestic transaction.

23.4.1 Member shall ensure that Domestic Processing of FIR is initiated and proceeded through UPI ID or through account number and IFSC.

23.4.2 Beneficiary Bank shall ensure that Domestic Processing of FIR transactions are processed only to KYC-compliant beneficiary bank accounts and ensure that complete audit trail of the remittance chain is maintained.

23.4.3 Member shall ensure usage of designated UPI identifiers including institution block and initiation mode, to appropriately identify domestic processing of FIR transactions.

23.5 UPI Payments using international mobile numbers

Users with international mobile numbers to be allowed to onboard and transact on UPI. It facilitates inclusion of Users with international mobile numbers within the UPI ecosystem, thereby extending UPI access beyond Indian mobile numbers.

23.5.1 Members shall ensure that UPI onboarding and transactions using international mobile numbers shall be allowed for country codes mentioned in Annexure B.

23.5.2 Members shall ensure adherence to all onboarding and transaction-level checks, including risk controls, cooling period, and other applicable safeguards under UPI guidelines.

24. Central Bank Digital Currency (CBDC) – RBI's Digital Rupee

RBI's Digital Rupee (CBDC) wallet holders can transact on the UPI QR acceptance network. A CBDC wallet User scans a standard UPI QR to pay, bringing Digital Rupee onto the existing UPI Merchant and P2P acceptance base without a separate CBDC-specific QR.

24.1 Member and UPI Application Provider shall allow only scan and pay via UPI QR for Person and for Merchant payments.

24.2 Members and UPI Application Provider shall not allow cash withdrawal, gallery share and pay, or any other method.

24.3 CBDC wallet issuer shall not allow wallet top-up from credit accounts.

24.4 Members and UPI Application Providers shall ensure that CBDC to UPI transaction have a distinct identification at two levels, the handle (@dr<bankname>) marks the transaction as CBDC-originated and a dedicated purpose code.

25. RuPay Credit Card on UPI

Linking of RuPay Credit Cards with UPI is permitted, enabling cardholders to link their RuPay credit card account to a UPI Application and use it across applicable UPI payment features through a Virtual Payment Address (VPA)/ UPI ID. This enhances User convenience by expanding the acceptance and usage of RuPay Credit Cards across the UPI ecosystem. Merchants benefit from increased User spending and participation in the digital credit ecosystem through acceptance of RuPay Credit Card transactions using existing UPI infrastructure, including QR codes.

RuPay Credit Card on UPI shall be used across UPI features and services including P2M transactions, EMI, UPI AutoPay, UPI Reserve Pay, UPI Biometric Authentication among others.

25.1 Credit card issuers shall comply with extant regulatory guidelines and only authorized credit card issuers shall be permitted.

25.2 Member shall support discovery and linking of eligible credit cards on UPI Application Provider and for making applicable Merchant transactions.

25.3 Member shall consider the device binding and UPI PIN setting process conducted during credit card onboarding on the application, as customer consent for credit card enablement for all types of transactions on UPI. For international transaction additional enablement on UPI, the existing process from the UPI Application shall apply.

25.4 UPI Application Provider, PSP and issuer shall ensure P2P, P2PM, card-to-card payments shall not be permitted. Member shall not permit transactions for any restricted categories as per extant regulatory guidelines.

25.5 Acquirer shall ensure that cash withdrawal at Merchants is not permitted.

25.6 Acquirer shall inform and educate Merchants to enable acceptance of credit cards and overdraft accounts through UPI. Acquirers shall also ensure transparency to Merchants as per extant Applicable Law.

25.7 Acquirers shall ensure overall compliance, monitoring and hygiene within the Merchant ecosystem, including tagging of MCCs and classification of online/offline Merchants in accordance with regulatory guidelines.

26. Credit Line on UPI (Credit on UPI)

UPI supports inclusion of pre-sanctioned credit lines as a source of funds. Credit on UPI shall provide a seamless, UPI enabled credit lifecycle experience for Users. As per regulatory guidelines the scope of UPI is expanded by inclusion of pre-sanctioned credit lines as a source of fund. Further, regulator has amended Master direction on Credit Facilities to ensure consistency in regulatory guidelines towards such products across banks.

26.1 The credit products that can be linked and used on UPI as Credit on UPI shall be categorised as either:

26.1.1 Interest Free Credit Line (CLIF): Credit facility with an interest free period wherein interest free payment can be made, subject to the payment of entire outstanding on or before the payment due date by the User.

26.1.2 Interest Bearing Credit Lines (CLIB): Credit facility wherein the interest will be accrued to the User from the date of transaction performed using the credit facility.

26.1.3 Credit on UPI shall be used across UPI features and services including P2M transactions, P2P transactions (CLIB), Equated Monthly Instalment (EMI), UPI AutoPay, UPI Reserve Pay, UPI Biometric Authentication amongst others.

26.2 Issuer shall comply with extant Applicable Laws for issuance and operations of such Credit accounts.

26.3 Member shall support discovery and linking of eligible credit accounts on UPI Application Provider and for making applicable Merchant transactions.

26.4 Device binding and UPI PIN setting conducted during credit line onboarding on UPI Application Provider shall include and be construed as user consent for credit line enablement and acceptance for all types of transactions on UPI.

26.5 Member shall not permit transactions for restricted categories as per extant regulations.

26.6 Issuer shall, as per its board approved policy, stipulate terms and conditions of use of such credit lines and ensure compliance with extant regulatory guidelines, bank policy, legal requirements and defined purpose of such CLIB offering.

26.7 Issuer shall approve or decline transactions initiated via UPI as per extant regulatory guidelines and defined purpose of credit.

26.8 Acquirer shall inform and educate merchants to enable merchants for Credit Line acceptance through UPI and ensure transparency.

26.9 Acquirer shall ensure overall compliance, monitoring and hygiene for Merchant ecosystem such as tagging of MCC and regulatory compliance.

26.10 Member shall refer Annexure F for features applicable for credit account types.

26.11 Members shall standardise the account sub type and account reference number (as per the detailed guidelines laid down in the product document) to harmonise the User experience, reducing friction at the point of payment, and enabling scalable adoption of Credit on UPI. Member and UPI Application Provider shall ensure the implementation by December 15, 2026.

27. Prepaid Payments Instruments on UPI (PPI on UPI)

PPI on UPI enables interoperability of PPIs on the UPI, allowing Users to make and receive payments seamlessly through UPI. A PPI Issuer shall enable holders of its full-KYC PPIs to make UPI payments or guided by extant regulatory guidelines as introduced from time to time.

27.1 PPI Issuer shall be a Payment Service Providers (PSP) in UPI with its own UPI Application.

27.2 PPI Issuer may also facilitate discovery of its full-KYC PPIs on third-party UPI Application.

27.3 A PPI Issuer, in its capacity as a PSP, shall not onboard Users of any bank or any other PPI Issuer.

27.4 PPI Issuer as a PSP shall comply with the prescribed regulatory requirements for authentication of UPI transactions initiated from its own UPI Application.

27.5 The extant UPI authentication process shall be followed in case of transaction initiated from PPIs through third-party UPI Application Providers.

28. e-RUPI Voucher

e-RUPI is a prepaid digital voucher that enables Governments, Corporates, and Individuals, acting as a sponsor, to issue benefits, incentives, or gifts to designated e-RUPI Beneficiary. The voucher may be issued as either a One-time use or Multiple use, depending on the applicable use case and shall be purpose-specific to ensure utilisation only for intended purpose by the designated e-RUPI beneficiary.

28.1 e-RUPI Issuer shall ensure that only Full-KYC compliant account holders, acting as sponsors, are authorized to initiate the issuance of One-time use (non-reloadable) or Multiple time use (reloadable/ non- reloadable) e-RUPI vouchers for Government and Corporate use cases.

28.2 For Individuals issued e-RUPI voucher, Payer PSP/ UPI Application Provider shall ensure that payment towards the issuance of One-time use (non-reloadable) or multiple time use (non- reloadable) e-RUPI vouchers shall be made from their Bank accounts upon successful AFA validation. Further, Remitter Bank shall ensure that payments for the issuance of e-RUPI vouchers are initiated by Users holding Full-KYC compliant accounts.

28.3 e-RUPI Issuer shall ensure that the e-RUPI voucher is issued with a maximum validity up-to one year (1 year) from the date of issuance.

28.4 e-RUPI Issuer shall ensure that e-RUPI voucher once issued, is not transferrable.

28.5 Payer PSP/ UPI Application Provider and e-RUPI Issuer shall ensure that e-RUPI vouchers are redeemed for Merchant transactions only.

28.6 Payer PSP/UPI Application Providers and e-RUPI Issuer shall ensure that e-RUPI voucher is not used for cash withdrawal, cash back, loan repayment, credit card bill payments, insurance, gold purchase, fund transfers, investment, capital market payments and wallet load transactions.

28.7 e-RUPI Issuer shall ensure that an e-RUPI voucher may be revoked at the request of the sponsor only until the beneficiary has successfully set UPI PIN for the voucher. Once the UPI PIN has been set, the voucher shall become irrevocable, and neither the Sponsor nor the e-RUPI Issuer shall be permitted to revoke the voucher.

28.8 The Payer PSP/UPI Application Providers and e-RUPI Issuer shall allow beneficiaries to discover and set a UPI PIN for any e-RUPI voucher via the UPI Application Provider.

28.9 For redemption of e-RUPI Vouchers issued by government entities, e-RUPI Issuer and Payee PSP shall support the e-RUPI beneficiary to perform redemption through scanning the SMS / Voucher QR Code. Payee PSP shall send the verification code to the beneficiary's mobile number and validate the same during redemption.

28.10 Payer PSP / UPI Application Providers and e-RUPI Issuer shall ensure that e-RUPI voucher issued by corporate and individual are redeemed through the UPI Application Provider only upon completion of Additional Factor of Authentication (AFA).

28.11 Payer PSP/UPI Application Provider shall ensure that, during e-RUPI voucher redemption, the voucher is presented as the default debit option where the Merchant Category Code (MCC) mapped to the voucher purpose code matches with the Payee's MCC. In cases where multiple eligible vouchers exist for the same purpose code and matching MCC, the voucher with the earliest expiry date shall be selected as the default debit option. UPI Application Provider shall allow beneficiary to change the debit option as per their choice and select other payment instruments.

PART IV – SETTLEMENT AND RECONCILIATION

29. Settlement

NPCI as the authorized payment system operator undertakes inter-bank / member settlement of payment transactions. The Members' settlement obligation arises once the transaction is successfully processed in UPI. The payment obligations and settlement instructions among the Members shall be determined through netting procedure, i.e. the net debit/credit position based on the total debit and credit transactions for a particular Member including disputes & adjustments, interchange fees, NPCI fees, charges, etc. Once the netting procedure is completed, the settlement shall be final and irrevocable.

For each settlement cycle, a Member may be in either a net debit position or a net credit position. In case of net debit position, the Member's payment obligation in respect to settlement shall arise towards other Members. As part of the settlement process, the settlement account of all the Members that are in net debit position is debited and settlement account of all the Members in net credit position is credited, through Multilateral Net Settlement Batch (MNSB) in the Real-Time Gross Settlement (RTGS) system. To effect this payment obligation, the Members who are in net debit position must ensure they maintain sufficient funds in their respective settlement accounts. The settlement cycles and time of settlement file posting in RTGS is given in Annexure E for reference.

The Sponsor Bank shall be responsible for fulfilling the payment obligations of its Sub-Members with respect to settlement. The net settlement amount payable by a Sub-Member is included as part of the settlement file of its Sponsor Bank while posting the MNSB file for settlement.

In case the settlement account of a Member having net debit position does not possess adequate funds, the Member shall be in breach of its payment obligations with respect to settlement, leading to a cascading effect on other Members' payment obligations and successful completion of the settlement. The settlement is governed under the Settlement Guarantee Mechanism communicated by NPCI from time to time.

Sponsor Banks shall manage Net Debit Cap (NDC) limits for itself and its Sub-Members transactions within the overall NDC limits approved by NPCI for the Sponsor Bank. The Sponsor Bank shall maintain adequate controls, approvals and governance around NDC limit management.

Members shall refer to and be guided by the Procedural Guidelines (PG) and Operating and Settlement Guidelines (OSG) for detailed settlement procedures, reports availability, operational processes and exception handling, for adherence.

30. Reconciliation

All Members are responsible for daily reconciliation of their UPI transactions. Members shall have process and systems for automated reconciliation for UPI transactions and shall accord top priority to carry out reconciliation. The Member shall follow the procedures set out in the UPI PG for reconciliation of declined, deemed-approved, timed-out and exception transactions.

PART V: DISPUTE MANAGEMENT MECHANISM

31. Dispute Management

Members are responsible for addressing and resolving the customer complaints raised for UPI transactions. Members shall set up and clearly communicate a dedicated and easily accessible grievance redressal mechanism for addressing such customer complaints. Members shall ensure that contact details for raising customer complaints are prominently displayed on their website and other channels. Complaints received by NPCI, if any, shall be redirected to the relevant Member for resolution.

Members shall address the customer complaint / transactions disputes using the dispute resolution mechanism made available by NPCI. Members shall comply with chargeback eligibility criteria, limits, timelines and dispute management process.

Members to abide by the regulatory guidelines on Harmonisation of Turn Around Time (TAT) and customer compensation for failed transactions using authorised payment systems and any other regulatory guidelines related to customer grievance redressal.

Members to refer and be guided by the UPI PG on UPI dispute management process.

32. Unified Dispute and Issue Resolution (UDIR)

32.1 Member and UPI Application Provider shall implement online dispute resolution process for handling and resolving complaints.

32.2 Member and UPI Application Provider shall implement UDIR in UPI for addressing pending transactions and facilitate Users to raise complaint for Merchants' transactions for service-related issues.

32.3 UPI proactively triggers an API to the Remitter/Beneficiary Bank for checking and updating the status of pending transactions debit reversal timeout or deemed (credit timeout) transactions. Remitter and Beneficiary Bank shall respond to this API on real-time and process reversals/credits respectively to their User.

32.4 For all complaints received by NPCI, the status shall first be checked in URCS. For pending transactions or transactions where no dispute has been raised, an API request shall be sent to the relevant Member. Remitter and Beneficiary Bank shall respond to this API on real-time and process reversals/credits to their User as applicable. Upon receipt of the Member's response, the status, dispute, or adjustment is updated in URCS and all relevant parties shall be notified. Remitter and Beneficiary Bank shall process manual credit to User accounts only after verifying if the amount was already reversed online or credited online. Pre-approved online functionality via 'refund API' (supporting partial and full refunds) shall be used by the Beneficiary Banks to process refunds for Merchant transactions. Since in pre-approved transactions the availability of funds is secured before the transaction is initiated, and as the debit leg is already assured, the further transaction is processed without being routed to the Remitter Bank.

32.5 Payer PSP shall enable raising of complaints from UPI Application, to display status of transaction and / or disputes, as and when updated in URCS using UDIR APIs and ensure adherence to velocity checks for API usage.

32.6 Member shall ensure necessary changes are done at switch and Member's Core Banking System (CBS) for supporting APIs for online status check and take appropriate action on pending transactions DRC or deemed transactions. To make necessary changes in the reconciliation and complaints handling process for facilitating UDIR process.

32.7 Member is expected to respond with appropriate actions for updating transaction status and resolving complaints.

32.8 Member shall have validation/ check process in their system to avoid duplicate processing in real-time as well as during reconciliation. For Online reversal response in Auto update API, Remitter Bank shall ensure that double credits are not passed in customer accounts for return (RET) cases (RET is where the Beneficiary Bank cannot process the credit to the User/customer account and returns the funds back to the Remitter).

32.9 Member live on UDIR shall not pass manual entries (credit/reversal) to User account for exceptions/pending transactions identified during reconciliation on the transaction date (T+0). Member to do so on T+1 day, after checking the latest settlement/adjustment reports and User account while passing manual entries, to avoid duplicate credit/reversals.

32.10 Payee PSP shall use the existing NPCI back-office (URCS) dispute management system to process refunds or extend the UDIR refund API to their Merchant platform to process pre-approved online refunds (partial or full amount). If the Payee PSP chooses to use any other system or channel to process refunds, they assume full liability for any issues arising from those transactions.

32.11 Payee PSP must provide the following information to merchants on a regular, periodic, or real-time basis:

i) Real time check transaction status option to the Merchant to check the status.

ii) Information/summary of transactions performed along with refund status.

Member to refer and adhere to the latest version of UDIR technical specifications and functional documents, including Operating Circulars and Procedural Guidelines issued from time to time.

33. UPI HELP – AI powered support for UPI payments

UPI HELP is introduced with the objective of enhancing User trust and confidence in UPI ecosystem, especially to assist Users on UPI payments. UPI HELP is powered by a proprietary financial domain-specific language model, to enhance User engagement by providing intelligent conversational support. It is a multilingual support platform designed to enhance support experience for Users. It enables Users to view transaction history, transaction status enquiries, raise and track complaints for pending transactions and merchant service-related issues, mandate management, etc. UPI HELP will continue to evolve, with ongoing enhancements, new use cases and capabilities to improve user support and overall convenience.

33.1 Member shall ensure all complaints received via this channel are acknowledged, registered, and resolved within the prescribed Turn Around Time (TAT) and other rules defined for grievance redressal and related actions as per the extant guidelines.

33.2 Member live on UDIR must consume complaints raised via UPI HELP and act promptly on auto-resolution mechanisms for transactions marked as pending or deemed via UDIR process, providing timely updates within stipulated TAT.

33.3 Remitter shall maintain consistent communication with Users regarding their complaints, referencing the Complaint Reference Number (CRN) and guiding them on the dispute status and further steps.

33.4 Upon Mandate action initiation (e.g., pause, resume, revoke) via UPI HELP, UPI Application Provider shall redirect Users to the appropriate confirmation or review screen as per the existing UPI AutoPay guidelines.

33.5 Member and UPI Application Provider shall ensure that data made available in UPI HELP shall be accessed or used (directly or indirectly), by Member of the payment system, only for the purpose of providing UPI HELP services to their Users and for no other purpose.

33.6 All roles and responsibilities of Member shall be applicable as per terms of participation including UPI System Requirement as issued by NPCI from time to time.

PART VI - COMPLIANCE AND SELF-ATTESTATION

34.1 Self-Attestation is a periodic compliance process through which Members are required to confirm their adherence to applicable UPI Procedural Guidelines (UPI PG), Operating and Settlement Guidelines (OSG), Technical Specification Documents (TSDs), Operating Circulars, Risk Management Directions (RMD), NPCI and UPI Brand Guidelines, UPI Information Security Compliance Framework, Error and Response Codes Document, UPI Application Providers checklist, Product Feature Document, Operating Circulars related to Pricing, UPI API usage guidelines and monitoring framework issued by NPCI.

34.2 Members shall submit the self-attestation through the prescribed NPCI portal on an annual basis or as and when required by NPCI.

PART VII - GENERAL

35.1 Amendments / Modifications

The Consolidated Circulars may be amended, modified, supplemented, suspended or withdrawn, in whole or in part, from time to time as deemed necessary, including for fulfilment of any operational, technical, risk, security, compliance or participant requirements specified herein. Such amendments shall be binding on all Members and UPI Application Providers from the relevant issue /effective date.

35.2 Audit and Records

Every Member, Sub-Member and system participant shall provide full cooperation and access to NPCI or its authorised personnel during any inspection or audit of the activities, systems, processes, controls and compliance of any participant in relation to the features/ services governed by this Circular and/or compliances under Applicable Law in relation to the payment system.

Every Member, Sub-Member and system participant shall maintain complete and accurate records relating to activities undertaken pursuant to this Circular and shall preserve such records for such period as may be prescribed by Applicable Law, regulation, as amended from time to time.

35.3 Requisition of Information

Every Member, Sub-Member and system participant shall provide, any information, records, books, registers, logs, data, correspondence, policies, agreements, reports, certifications, transaction details, system-generated records, audit trails, customer consents, or other documents and materials that may be required from time to time.

Annexure A – Glossary

In this Consolidated Circular, unless the context requires otherwise, the following terms have the meanings set out below. Terms used but not defined here shall have the same meaning as assigned to it under the PSS Act, 2007 and / or any other extant Applicable Law.

Term	Definition
Acquirer or Acquiring Bank	A Bank or financial institution that onboards / signs a Merchant and facilitates the collection of payments for such Merchant by enabling acceptance of UPI transactions through QR, Point of Sale (PoS) terminals, e-Commerce platforms and other channels. In the context of UPI, the Acquirer refers to the Payee PSP.
Applicable Law	Means and includes any statute, law, regulation, circular, notification, ordinance, rule, judgment, rule of law, order, decree, clearance, approval, authorization, directive, guideline, code, standard and manual, policy, requirement, or other government restriction or any similar form of decision, or determination by, or any interpretation or administration of any of the foregoing by, any statutory or judicial or Government Authority or regulatory authority, issued by any authority under Republic of India and applicable in each country / jurisdiction where the UPI transaction takes place, as amended, modified, supplemented, re-enacted, or replaced from time to time.
Beneficiary Bank or Beneficiary PPI	A Bank or non-bank entity that holds the recipient's account and receives the credited funds in respect of a UPI transaction.
Bharat QR	An interoperable, standards-based Quick Response (QR) code payment solution enabling customers to make card or UPI based payments by scanning the QR code displayed by a Merchant.
Business Correspondent (BC)	A person or organization appointed by a bank or financial institution to provide banking services on behalf of such institution.
Collect Request	A recipient-initiated UPI transaction through which the Payee PSP initiates a request to collect funds from the person making payment.
Delegation	An authorisation granted by the Primary User to the Secondary User to undertake UPI transaction through/ using UPI Circle.
Dynamic QR	A Quick Response (QR) code containing recipient's / payee's payment details, generated uniquely for each transaction.
End Beneficiary	In case of Person-to-Merchant (P2M) or Person-to-Person (P2P) transaction, the Merchant or person receiving funds in consideration of goods supplied or service rendered.
e-RUPI Issuer	A Bank or an entity authorised to issue a Prepaid Payment Instrument (PPI) and initiates a request for the creation of an e-RUPI voucher.

Term	Definition
e-RUPI Voucher	A prepaid digital voucher issued to a recipient / beneficiary for a specified purpose and redeemable through UPI at designated Merchants.
Full Delegation	An authorisation granted by the Primary User to one or more Secondary Users and/or any other UPI ID(s) identified by the Primary User, enabling such person(s) or UPI ID(s) to initiate and complete UPI transactions in accordance with prescribed spending limits.
Intent	A messaging object or deep link, supported by the operating system of the User's mobile device, which is used to request an action from UPI Applications installed on such device and facilitate communication between the Merchant's application and UPI Applications.
LITE Auto Top-Up	A Mandate-based feature that enables a User to automatically replenish a UPI LITE wallet from an account linked to such UPI LITE wallet when the wallet balance falls below a specified threshold.
LITE Reference Number (LRN)	LITE Reference Number (LRN) means a unique reference number assigned to each UPI LITE account for identification and reconciliation purposes.
Mandate	An instruction given by a User to the Remitter Bank to debit funds from, or earmark/block funds in, an account linked to the User's UPI ID, either on a one-time or recurring basis.
Mandate Validity Period	The period for which a Mandate remains active, as specified / selected by the User, after which such Mandate shall be deemed expired and invalid.
Member	A bank or financial institution that pursuant to a contractual arrangement with NPCI participates in UPI and provisions UPI features/ services to its customers and Users and is on-boarded in UPI as an Issuer and/or PSP. Member is a bank, PPI Issuer and non-banking financial company, including a Sub-Member, payments bank.
Merchant	A person, entity or a marketplace that sells goods, provides services, or offers investment products, and includes exporters and overseas sellers, among others.
Merchant Category Code (MCC)	An identifier used by Acquirer to classify Merchants into specific categories based on the nature of their business, trade or services.
Numeric UPI ID Mapper	A centralized system that enlists/maps a UPI Number (numeric UPI ID) to its corresponding UPI ID and identifies the relevant PSP that has issued such UPI ID for the purpose of routing the transaction.
Operating Circulars	The circular issued by NPCI as may be amended, modified, supplemented or replaced from time to time and includes the Consolidated Circular.

Term	Definition
Partial Delegation	A delegation mode under UPI Circle wherein the Secondary User has the authority to initiate payment requests to the Primary User for authorization.
Payee PSP	The PSP through which any person or Merchant is on-boarded onto UPI as a recipient for the purpose of receiving payments through UPI.
Payer PSP	The PSP through which the User or Merchant is on-boarded onto UPI for the purpose of making payments through UPI.
Payment Aggregator	An entity that facilitates aggregation of payments made to Merchants through one or more payment channels via a Merchant's interface (physical or virtual) for the purchase of goods, services or investment products, and subsequently, settles the collected funds to such Merchants.
Payment Gateway	An entity that provides technology infrastructure for routing and processing payment transactions without handling customer funds.
Payment Service Provider (PSP)	A Member that onboards a User onto UPI by issuing UPI ID to it and processes UPI transactions made by the User through the UPI Application of the Member or its TPAP or any other technology-based system / solution. PSP can be primary PSP, secondary PSP, Payer PSP or Payee PSP.
Peak Hours	The periods during which UPI transactions reach the highest transaction volumes per second, currently observed between 10:00 hours to 13:00 hours and from 17:00 hours to 21:30 hours.
Penny Drop	A penny drop transaction is a small-value transaction made to an account to verify the validity and ownership of an account.
Prepaid Payment Instrument (PPI)	An instrument that facilitates the purchase of goods and services, financial services, remittance services and other permitted transactions against the value stored therein.
Prepaid Payment Instrument (PPI) Issuer	A bank or financial institution authorised to issue and maintain Prepaid Payment Instrument (PPI) to its User.
Pre-Transaction Notification	A notification sent by the Issuer to the registered mobile number or email address of the User in respect of an AutoPay transaction at least 24 hours prior to the scheduled debit. Also, referred to as Pre-Debit Notification.
Primary User	An User who authorizes a Secondary User or IoT device identified by the Primary User to undertake transactions through UPI Circle.
Remitter Bank	A Bank or financial institution that maintains the payer's account linked to UPI, authenticates the payer and debits such account on receipt of a valid UPI transaction request. In the context of UPI, the Remitter Bank and issuer are the same.

Term	Definition
Secondary User	A person authorized by a Primary User to make payments from their account linked to UPI using UPI Circle.
Sponsor Bank	A bank that undertakes to honour the Settlement obligation of a Sub-Member in relation to Sub-Member's transactions processed through UPI by allowing debit and credit of funds in the Settlement Account of the Sponsor Bank.
Static QR	A QR code containing the beneficiary's payment details that is not generated for a specific transaction and may be used for multiple UPI transactions.
Sub-Member	A Member who is not a member of the Real Time Gross Settlement system of RBI.
Third Party Application Provider (TPAP)	An entity engaged by PSP as its application provider to provide a UPI enabled mobile application for User onboarding, facilitation of UPI transactions and provision of related services to their Users, and which is approved by NPCI to participate in UPI as a TPAP through such PSP.
Unified Dispute and Issue Resolution (UDIR)	An automated, single-channel grievance redressal system designed to facilitate seamless resolution of User complaints and issues relating to pending or disputed transactions.
Unique Mandate Number (UMN)	A unique identifier assigned to each successfully registered Mandate.
UPI Application	An application provided to the User by a PSP, either directly or through a TPAP, to make UPI based transactions and avail of related services.
UPI Application Provider	A PSP or TPAP that offers its UPI Application to its Users.
UPI AutoPay	A Mandate registered by a User to enable automated debits for recurring payments.
UPI ID or Virtual Payment Address (VPA)	A unique identifier (for example, username@pspname) created and assigned to a User or Merchant for the purpose of routing UPI transactions to or from the account linked to such identifier.
UPI QR	An interoperable Quick Response (QR) code payment solution that enables User to make payments through UPI by scanning a QR code displayed by a Merchant, subject to applicable UPI rules and regulations/guidelines.
UPI System Requirements	UPI Procedural Guidelines (UPI PG), Operating and Settlement Guidelines (OSG), Technical Specification Documents (TSDs), Operating Circulars, Risk Management Directions (RMD), NPCI and UPI Brand Guidelines, UPI Information Security Compliance Framework, Error and Response Codes Document, UPI Application Providers checklist, Product Feature Document, Operating Circulars related to Pricing, UPI API usage guidelines and monitoring framework issued by NPCI, and /

Term	Definition
	or any other document issued by NPCI in relation to the operation of the UPI payment system.
User	A person or entity that undertakes financial or non-financial transactions through UPI and is a customer of a Member and/or UPI Application Provider, including a Merchant.
Verified Merchant	A merchant categorised by a PSP as verified following the completion of due diligence by the PSP and inclusion in the Verified Address Entries (VAE) list.

Annexure B – List of Country Code and Currency Codes

List of Countries enabled for UPI Global Acceptance with Country Codes and Currency Codes

Sr. No.	Country	Country Code	Transaction currency Code
1	Nepal	NP	NPR
2	Singapore	SG	SGD
3	Thailand	TH	THB
4	Malaysia	MY	MYR
5	Hong Kong	HK	HKD
6	Philippines	PH	PHP
7	South Korea	KR	KRW
8	Japan	JP	JPY
9	Indonesia	ID	IDR
10	Vietnam	VN	VND
11	United Arab Emirates	AE	AED
12	Sri Lanka	LK	LKR
13	United Kingdom	GB	GBP
14	Egypt	EG	EGP
15	United States of America	US	USD
16	Mauritius	MU	MUR
17	Bhutan	BT	BTN
18	Australia	AU	AUD
19	Saudi Arabia	SA	SAR
20	Qatar	QA	QAR
21	Austria	AT	EUR
22	Belgium	BE	EUR
23	Croatia	HR	EUR
24	Cyprus	CY	EUR
25	Estonia	EE	EUR
26	Finland	FI	EUR
27	France	FR	EUR
28	Germany	DE	EUR
29	Greece	GR	EUR
30	Ireland	IE	EUR
31	Italy	IT	EUR
32	Latvia	LV	EUR
33	Lithuania	LT	EUR
34	Luxembourg	LU	EUR

Sr. No.	Country	Country Code	Transaction currency Code
35	Malta	MT	EUR
36	Netherlands	NL	EUR
37	Portugal	PT	EUR
38	Slovakia	SK	EUR
39	Slovenia	SI	EUR
40	Spain	ES	EUR
41	Bahrain	BH	BHD
42	Cambodia	KH	KHR
43	Canada	CA	CAD
44	Kuwait	KW	KWD
45	New Zealand	NZ	NZD
46	Oman	OM	OMR
47	South Africa	ZA	ZAR
48	Switzerland	CH	CHF

List of Countries enabled for Reverse Acceptance with Country Codes and Currency Codes

Sr. No.	Country	Country Code	Transaction currency Code
1	Bhutan	BT	BTN
2	Mauritius	MU	MUR
3	Nepal	NP	NPR
4	United Kingdom (UK)	GB	GBP

List of international mobile number country codes allowed to onboard and transact on UPI

Sr. No.	Country Name	Country Code
1	Singapore	+65
2	Australia	+61
3	Canada	+1
4	Hong Kong	+852
5	Oman	+968
6	Qatar	+974
7	United States of America	+1
8	Saudi Arabia	+966
9	United Arab Emirates	+971
10	United Kingdom	+44
11	Malaysia	+60
12	France	+33
13	Bahrain	+973
14	Bhutan	+975
15	Brazil	+55
16	Germany	+49
17	Greece	+30
18	Ireland	+353
19	Italy	+39
20	Japan	+81
21	Kuwait	+965
22	Maldives	+960
23	Nepal	+977
24	Netherlands	+31
25	New Zealand	+64
26	Philippines	+63
27	Portugal	+351

Sr. No.	Country Name	Country Code
28	South Africa	+27
29	Spain	+34
30	Sweden	+46
31	Thailand	+66

Annexure C – Errors/Conditions where check transaction API shall not be initiated

Sr. No.	Error / Condition
1	Connection timeout
2	Connection refused
3	No route to host
4	Unknown host
5	Port unreachable
6	TLS handshake error
7	HTTP Status code: 501
8	HTTP Status code: 503
9	HTTP Status code: 403
10	HTTP Status code: 417
11	HTTP Status code: 404
12	HTTP Status code: 429
13	HTTP Status code: 413
14	Any Negative ACK from NPCI
15	Transaction Success/Failure confirmation from NPCI

Annexure D – Indicative Reference list of keywords not allowed for individuals

Product Name	Definition	Example	Source
Designation	Includes all the official title in public and private sector	CEO, CMO, PM, PMO, Finance Minister, etc	-
Bank	Includes all bank names and designations related to banks	Axis bank, SBI, branch manager, branch officer	Banks registered with RBI
Institution	All public institutions working directly or indirectly with the government	NITI Aayog, NPCI, etc	Institutions registered with GOI
Brand Name	All brands registered with trademark legally binding	Mc Donalds, Levis, Ford, etc	Brands registered with Trademark Office
Financial Institutions	All institutions which are related to banking/lending/BFSI/Insurance/NBFC/Chit fund houses/Clearing houses/Depository Participants	NSDL, CDSL, Indiabulls, SKS Finance, LIC, etc	Financial Institutions registered with SEBI, RBI and CAG
Corporates	All domestic and MNC companies registered with ROC	Airtel, MRF, Britannia, etc	ROC
NGOs	All domestic and foreign NGOs registered with ROC	Being Human, etc	ROC
Trusts	All trusts registered with Charity Commissioners office	Siddhivinayak Trust, Tirupati Balaji Trust	Charity Commissioners office
Universities	All public and deemed private educational institutions	IIT, IIM, NMIMS, Delhi University, etc	List of approved educational institutions from Education Ministry
Government Offices, departments	All public offices reporting to existing government structure	BMC, Passport office, Secretary departments	List of institutions approved by government
Slangs (Abusive words)	All and any words which are abusive/offensive in nature	As per English and Hindi dictionary	As per Oxford and Hindi dictionary
Websites	All websites registered under World Wide Web	Google, Facebook, etc	Registered domains under WWW
Political Parties	All political parties registered with Election Commission of India	BJP, UPA, NDA, etc	Registered with EC

Product Name	Definition	Example	Source
Government Scheme or Yojna	All registered government schemes	Jan Dhan Yojna, Swachh Bharat Abhiyaan, etc	Approved by Government
Awards (Government, Private or Any)	All official government awards	Bharat Ratna, Arjuna Award, etc	Presented by Government
Enterprises owned by Government	Organizations owned by State, UT and Central Government	ISRO, DRDO, India Post, BEST, etc	-

Indicative List not to be allowed for Users

Websites	Miscellaneous	Corporate Designations	Govt. Office/Body
Google	Black Money	CEO	BMC
Facebook	NPCI	CMO	Municipality
Twitter	UPI	Chairman	PMO
LinkedIn	Branch Manager	CXO	RBI
Snapdeal	Manager	CTO	SEBI
Flipkart	IT	CIO	FEMA
bookmyshow	ITR	COO	CBI
Paytm	Income tax	AVP	Police
mobikwik	bank	President	Supreme court
Amazon	Indian Army	Vice President	Passport
Alibaba	Indian Navy	GM, DM, AGM	Prime Minister
Alipay	Indian Air force	-	Prime Minister Fund
pepperfry	Defence	-	LIC
rentomojo	Pandemic	-	LIC INDIA
instagram	Covid19	-	NABARD
snapchat	Corona Virus	-	IRDA
-	Beinghuman	-	-
-	Red Cross	-	-
-	WHO	-	-
-	UNICEF	-	-
-	UNESCO	-	-
-	Disaster Relief fund	-	-
-	Swachchhbharat	-	-
-	KCC	-	-
-	AMFI	-	-
-	IIBF	-	-
-	IBA	-	-

Annexure E – UPI Settlement Cycles

Cycle No.	From Time	To Time	Duration (Hrs)
1	21:00	00:00	03:00
2	00:00	05:00	05:00
3	05:00	07:00	02:00
4	07:00	09:00	02:00
5	09:00	11:00	02:00
6	11:00	13:00	02:00
7	13:00	15:00	02:00
8	15:00	17:00	02:00
9	17:00	19:00	02:00
10	19:00	21:00	02:00
DC1(Dispute/Adjustment cycle)	00:00	16:00	16:00
DC2(Dispute/Adjustment cycle)	16:00	00:00	08:00

Note:

The posting of settlements as mentioned above in Sr. 1 & DC2 shall commence from 4:00 am in RTGS settlement account of the Members on all days of the year (excluding RTGS holiday, if any).

The posting of settlements of all other settlement cycles mentioned above shall commence after the cut-off time e.g. posting of cycle 2 shall start from 5:00 am, in the RTGS settlement account of the members on all days of the year (excluding RTGS holiday, if any).

ATM Interoperable Cash Deposit (ICD) transactions using UPI are settled once a day i.e. transactions from 00:00 to 00:00 hours are settled through a separate settlement in UPI URCS; For detailed Settlement and Dispute management procedures, Members to refer relevant guidelines in NFS OSG.

Annexure F – Features allowed on Credit Accounts

Particular	RuPay Credit Card on UPI	Interest Free Credit Lines (CLIF)	Interest Bearing Credit Lines (CLIB)
P2M transactions	Allowed	Allowed	Allowed as per end use of credit defined by Issuer
P2P, Self Transfer, Account + IFSC, Mobile Number based transactions	Not Allowed	Not Allowed	Allowed as per end use of credit defined by Issuer
P2PM transaction	Not Allowed	Not Allowed	Allowed as per end use of credit defined by Issuer
UPI ICCW	Not Allowed	Not Allowed	Allowed as per end use of credit defined by Issuer
UPI AutoPay	Allowed	Allowed	Allowed
UPI Reserve Pay	Allowed	Allowed	Allowed
Aadhaar OTP	Allowed	Allowed	Allowed
UPI 123Pay	Allowed	Allowed	Allowed
UPI Tap & Pay	Allowed	Allowed	Allowed
UPI Multi-signatory account	Not Allowed	Not Allowed	Not Allowed
Equated Monthly Instalment (EMI)	Allowed	Allowed	Allowed
UPI One Time Mandate	Allowed	Allowed	Allowed
UPI Plug-In	Allowed	Allowed	Allowed
UPI LITE	Not Allowed	Not Allowed	Not Allowed
UPI Circle	Not Allowed	Not Allowed	Not Allowed
UDIR/ UPI Help	Allowed	Allowed	Allowed
Inward Credit to VPA	Allowed for MCC 5969	Allowed for MCC 5969	Allowed
UPI International	Allowed	Not Allowed	Not Allowed
Restricted MCC	0000,4829,5413,6010,6011,6012,6013,6051,6211,7322,7407,7408,7409,7800,7801,7802,7995,9406	0000,4829,5413,6010,6011,6012,6013,6051,6211,7322,7407,7408,7409,7800,7801,7802,7995,9406	4829, 5413, 6010, 6011, 6012, 6051, 6211, 7322, 7408, 7409, 7800, 7801, 7802, 7995, 9406

Annexure G – List of withdrawn UPI Operating Circulars (OC)

Sr. No.	OC Number	OC Name
1	OC 1	Enablement of UPI for 1000 Employees
2	OC 2	Prerequisites for UPI customer launch
3	OC 4	Compliance with NPCI circulars and Procedural Guidelines of UPI
4	OC 8	Addendum to Circular for implementing UPI 1.5 changes
5	OC 11	Urgent enablement of reading/generating dynamic QR code
6	OC 12	Revision in benchmarking criteria of UPI system/interface of member banks.
7	OC 13	Compliance to merchant onboarding and SDK guidelines checklist
8	OC 15	UPI Merchant SDK: Specific requirements & Compliance
9	OC 20	Assigning exclusive MCC for Life Insurance Corporation of India (LIC)
10	OC 21	Usage of BHIM by bank's UPI PSP App
11	OC 22	Launch of Referral and Merchant Cashback scheme for BHIM users
12	OC 25	Discontinuing Services on USSD 1.0 system
13	OC 27	Inclusion of UPI Banks in BHIM Merchant Cashback and Referral Bonus Scheme
14	OC 35	Guidelines for positioning of UPI/ BHIM logo as payment mode at merchant location (offline and online)
15	OC 37	Banks PSP apps and third party apps compliance to UPI Deep linking specs 1.5.1
16	OC 42	Enhanced penalty for not updating TCC, RET, DRC & RRC after T+1 working days
17	OC 46	BHIM UPI branding at all UPI enabled apps and merchants
18	OC 50	Introduction of Bill Pay functionality (BBPS) on BHIM App
19	OC 52	Modification of BHIM incentive scheme for individuals and withdrawal of BHIM incentive scheme for merchants
20	OC 53	Compliance to the Sec 42A, Rule 3 and 7 of Information Technology Act,2000
21	OC 54	Regarding removal of Pay to Aadhaar functionality in UPI and IMPS
22	OC 61	UPI transaction frequency limit revised to 10 transactions for P2P w.e.f October 21, 2018
23	OC 63	Migration to UPI 2.0 by 31st March 2019
24	OC 71	Enhancement of per transaction limit to Rs 2.Lakhs for UPI based ASBA
25	OC 74	UPI Compliance guidelines

Sr. No.	OC Number	OC Name
26	OC 86	Addendum to RMD 001
27	OC 87	Indicative Guidelines for System Audit Report (SAR) on Data Localization (DL)
28	OC 89	Customer on-boarding on iOS based devices
29	OC 112	UPI Prepaid Voucher
30	OC 117	International merchant payments acceptance through UPI - UPI Global
31	OC 121	Changes in UPI raw data file
32	OC 126	Introduction of additional settlement cycles for UPI from 6 to 8.
33	OC 132	Safeguarding UPI ecosystem & revision of trnx limit
34	OC 137	Revised timeline for enablement of customer onboarding on UPI through Aadhaar OTP Authentication.
35	OC 152	Revised timelines on Changes in UPI raw file
36	OC 157	UPI Raw File version 3.0
37	OC 159	Guidelines on volume cap for Third Party App Providers (TPAPs) in UPI
38	OC 185	Implementation of ₹5 Lakh limit per transaction for specific categories in UPI
39	OC 187	UPI reporting requirements (Acquiring entities, UPI Apps & key merchants)
40	OC 115D	Addendum to Numeric UPI ID Mapper on Revised Timeline
41	OC 116A	Addendum to “Aadhaar OTP Authentication in lieu of Debit Card for Customer Onboarding on Unified Payments Interface (UPI)” on revised timeline
42	OC 133A	Addendum to OC 133 - Addition of Initiation Mode and Channel identifiers for new use cases
43	OC 59	Change of production IP of RGCS for UPI