



भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

**PROCEDURAL
GUIDELINES
FOR
AADHAAR ENABLE
PAYMENT SYSTEM**

VERSION 2.0

Introduction

Purpose

Aadhaar Enabled Payment System Procedural Guidelines (AePS-PG) is a procedural document that defines the guidelines for the members of the AePS to follow. It mandates all the members on the AePS to follow certain standard procedures to ensure smooth, secure, and effective operation of the network.

Audience

AePS-PG is to be used by all the members participating in the AePS and relevant departments at NPCI

Contents

AePS-PG contains detailed information on procedural guidelines for the members of the AePS group of services to follow. The information is organized in a manner to enable users to swiftly and easily identify the piece of information they need. The information is divided into eleven sections, with the eleventh section covering the annexures. The table of contents clearly elucidates all information in AePS-PG through a numbered section-wise break up. Circulars issued from time to time forms an integral part of AePS-PG

Amendment History

Sr. No.	Version Number	Summary of Changes	Change Month & Year
1	1.4	Initial Version	January, 2011
2	2.0	<ul style="list-style-type: none"> • Definition section is been added for the terminologies used in PG. • A brief of Customers in AePS is added to PG. • UIDAI's authentication operating model is added • Terms of Membership is modified for Non-NFS members. • Termination criteria/s are added in termination of services section • Brief about BHIM Aadhaar Pay is added • Introduction of SHG dual authentication and Refund transaction in BHIM Aadhaar Pay are added • Additional roles are added in roles and obligation for acquirers and issuers • AePS steering committee section is added 	September,2019

Contents

Definitions	i
UIDAI & Aadhaar related terms & Definition	i
NPCI related terms & definition	ii
Abbreviations	1
1 Introduction	2
2 Scope & Objective	3
3 Customers in AePS.....	4
4 Authentication operating Model.....	5
5 Membership	7
5.1 Terms of membership	7
5.2 Certification.....	8
5.3 Member Notifications	8
5.4 Termination of services.....	9
6 Products & Services.....	10
6.1 Aadhaar Authentication/ ONUS.....	11
6.2 Aadhaar enabled interbank (Off-us) Transactions	11
6.2.1 Balance Enquiry.....	11
6.2.2 Cash Withdrawal.....	12
6.2.3 Cash Deposit	12
6.2.4 Aadhaar to Aadhaar Funds Transfer	12
6.2.5 Mini statement	13
6.2.6 SHG Dual Authentication Transactions	13
6.3 BHIM Aadhaar	14
6.4 Best Finger Detection	15
6.5 eKYC transaction.....	15
6.6 Demographic Authentication	15
7 Roles & Obligation of members.....	16
7.1 Acquirer Bank shall be responsible for the following:	16
7.2 Issuer Bank shall be responsible for the following	17
8 AePS Steering Committee	18

8.1	Composition of Steering Committee.....	18
8.2	Functions of Steering Committee	18
8.3	Nomination and Terms of office	19
8.4	Frequency of meetings & Quorum	19
8.5	Decision making	20
8.6	Functions of members	20
8.7	Functions of Chair.....	20
9	Governance of AePS ecosystem	20
9.1	AePS group of Services Availability	20
9.2	Audit by NPCI	20
9.3	NPCI ASA liability	21
9.4	Non-Disclosure Agreement	21
9.5	Indemnification.....	21
9.6	Prohibition to Use NPCI Logo/ Trademark /Network	21
9.7	Penalty or Fine.....	22
9.8	Deviation from AePS and/or eKYC Service Operating Procedures	22
9.9	Pending Dues	22
9.10	Invoicing	22
9.11	Compliance to Reserve Bank of India Guidelines	22
9.12	Amendment to the Procedural Guidelines.....	23
9.13	KYC/ AML Compliance as per RBI guidelines.....	23
10	Components, Communication and Settlement.....	23
10.1	Interbank Settlements and Net Debit Cap (NDC)	23
10.2	Choice of Connectivity	24
10.3	Message Formats	24
10.4	Transaction Logging	25
10.5	Reports and Reconciliation	25
10.6	AePS Dispute Management System and Exceptions handling.....	25
10.7	Customer Complaints- change as per AePS.....	26
	Annexure-I	27
	Annexure-II	29
	Annexure-III	30

Annexure-IV	36
Annexure-V	37
Annexure-VI	41

Definitions

UIDAI & Aadhaar related terms & Definition

Aadhaar Act: An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto.

Aadhaar Number/UID: It means an identification number issued to an individual under sub-section (3) of section 3, & includes any alternative virtual identity generated under sub-section (4) of that section of Aadhaar act.

Authentication Devices: Authentication devices are host devices/electronic actors that form a critical link in the Aadhaar authentication ecosystem. These devices collect personal identity data (PID) from Aadhaar number holders, prepare the information for transmission, transmit the authentication packets for authentication and receive the authentication results. Examples of authentication devices include form factors ranging from desktop PCs, laptops, kiosks to Point-of-Sale (PoS)/handheld mobile devices (microATMs) and tablets. Such devices are expected to be used for a variety of purposes specific to every requesting entity's requirements.

Authentication Services: Aadhaar Authentication means the process by which the Aadhaar number along with the demographic information or biometric information of a Aadhaar number holder is submitted to the Central Identities Data Repository (CIDR) for its verification and such repository verifies the correctness, or the lack thereof, on the basis of the information available with it.

Authentication Service Agency (ASA): ASAs are agencies that have established secure leased line connectivity with the UIDAI Database (CIDR) in compliance with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies for Authentication Services.

Authentication User Agency (AUA): Authentication User Agency (AUA) is an entity engaged in providing Aadhaar Enabled Services to Aadhaar number Holder, using the authentication as facilitated by the Authentication Service Agency (ASA).

UIDAI: The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016") on 12 July 2016 by the Government of India, under the Ministry of Electronics and Information Technology (MeitY).

Virtual ID: VID is a temporary, revocable 16-digit random number mapped with the Aadhaar number. VID can be used in lieu of Aadhaar number whenever authentication or e-KYC services are performed. Authentication may be performed using VID in a manner similar to using Aadhaar number. It is not possible to derive Aadhaar number from VID.

NPCI related terms & definition

Acquirer Bank: Acquirer bank within the scope of AePS is the one that allows its infrastructure (terminal, BC services and cash) to be used by customer of some other bank.

Customer: Customer shall refer to an Aadhaar enabled account holder of a bank, looking for to certain banking services.

Issuer Bank: Issuer Bank within the scope of AePS is one that has an Aadhaar enabled account of a transaction initiating customer held with it.

Issuer Identification Number – IIN: The IIN shall be a six digit number which shall be allotted to a bank upon an application to NPCI from the Bank. IIN shall act as the identity for issuing Bank.

Member: Member shall be any entity willing to avail AePS & allied services of NPCI, Member should have a valid and subsisting Authentication User Agency (AUA) and KYC User Agency (KUA) Agreement with UIDAI.

Micro-ATM: A Point of Sale (POS) device used by a Business Correspondent for handling customer initiated cash and transfer transactions. It is an example of authentication device utilizing banking services.

National Payments Corporation of India [NPCI]: NPCI is an umbrella organization for operating retail payments and settlement systems in India, Founded in 2008, NPCI is a not-for-profit organization registered under section 8 of the Companies Act 2013. The organization is owned by a consortium of major banks.

Off-us Transactions: A type of transaction where customer utilizes infrastructure of some other bank to perform transaction for his/her bank.

Onus Transactions: An intra-bank (On-us) transaction is one where an Aadhaar initiated transaction has effects only in accounts within one and the same Bank.

Reserve Bank of India [RBI]: The Reserve Bank of India (RBI) is the central bank of India, which was established on April 1, 1935, under the Reserve Bank of India Act. The Reserve Bank of India uses monetary policy to create financial stability in India, and it is charged with regulating the country's currency and credit systems.

Transaction receipt: For all transactions whether intra-bank or interbank, a Transaction Receipt shall be printed and handed over to a customer as a transaction record with its finality status, by the BC/merchant through whom the transaction was initiated.

Abbreviations

1. AML: Anti Money Laundering
2. API: Application Programming Interface
3. ATM: Automated Teller Machine
4. AUA: Authentication User Agency
5. ASA: Authentication Service Agency
6. BFD: Best Finger Detection
7. DMS: Dispute Management System - an on-line application for resolving disputes
8. DN: Data Navigator – A New Version of Dispute Management System
9. e-KYC: electronic Know Your Customer service
10. KYC: Know Your Customer
11. KUA: KYC User Agency
12. KSA: KYC Service Agency
13. NACH: National Automated Clearing House of NPCI
14. NFS: National Financial Switch of NPCI
15. NPCI: National Payments Corporation of India.
16. NPCINET: A closed loop secure private network by NPCI
17. NREGA: National Rural Employment Guarantee Act
18. OTP: One Time Password
19. POS: Point of Sale
20. POI: Proof of Identity
21. POA: Proof of Address
22. RBI: Reserve Bank of India
23. RTGS: Real Time Gross Settlement
24. SGF: Settlement Guarantee Fund
25. SHG: Self Helped Group
26. UIDAI: Unique Identification Authority of India

1 Introduction

In order to further speed track Financial Inclusion in the country, two Working Groups were constituted by RBI on MicroATM standards and Central Infrastructure & Connectivity for Aadhaar based financial inclusion transactions with members representing RBI, Unique Identification Authority of India, NPCI, Institute for Development and Research in Banking Technology and some special invitees representing banks and research institutions.

The working group on MicroATM standards & Central Infrastructure & Connectivity has submitted its report to RBI. As a part of the working group it was proposed to conduct a Lab level Proof of concept (PoC), integrating the authentication & encryption standards of UIDAI, to test the efficacy of MicroATM standards and transactions using Aadhaar before they are put to actual use. The PoC was successfully demonstrated at various venues.

The purpose of Authentication is to enable Aadhaar-holders to prove their identity and for service providers to confirm the resident's identity claim in order to provide services and give access to benefits. Aadhaar Authentication shall make life simpler for the resident as it is meant to be a convenient system to prove one's identity without having to provide identity proof documents whenever a resident seeks a service. Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data such as biometric/demographic information is submitted to UIDAI (Central Identities Data Repository-CIDR) for matching, following which the UIDAI verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it. UIDAI confirms either proof of identity or verifies the information provided by the resident based on the data available at the time of Authentication. To protect resident's privacy, Aadhaar authentication service responds only with a "Yes / No" and no Personal Identity Information (PII) is returned as part of the response. In order to facilitate financial inclusion objective of GOI (Government of India) leveraging Aadhaar authentication through BC channel, NPCI formulated Aadhaar enabled Payment System (AePS).

Aadhaar Authentication system supports the following Authentication types:

- ✓ Biometric Matching
 - a. Finger Print Authentication
 - b. IRIS Authentication
- ✓ Demographic Matching
- ✓ Additional features such as One-Time-Password (OTP)

AePS is a bank led model which allows online interoperable financial inclusion transaction at PoS (MicroATM) through the Business correspondent of any bank using the Aadhaar/Virtual ID authentication. AePS allows you to do seven types of transactions.

- ✓ Balance Enquiry
- ✓ Cash Withdrawal
- ✓ Cash Deposit
- ✓ Aadhaar to Aadhaar Fund Transfer

- ✓ Mini Statement
- ✓ Purchase
- ✓ Refund transaction [Yet to be launched as on 11th Feb'19]

The only inputs required for a customer to do a transaction under this scenario are:-

- ✓ IIN (Identifying the Bank to which the customer is associated)
- ✓ Aadhaar Number
- ✓ Biometric captured during their enrollment
- ✓ Transaction Type (If needed)

Any resident of India having his/her Aadhaar number linked to a bank account can participate in AePS service. Hereafter, such accounts have been referred to as Aadhaar enabled bank account. AePS service can be accessed at any biometric enabled touch point viz, mobile application/Kiosk/Micro-ATM with certified or any form factor along with the STQC standards.

2 Scope & Objective

- a) To empower a bank customer to use Aadhaar number/Virtual Id to access his/ her respective Aadhaar enabled bank account and perform basic banking transactions like Balance Enquiry, Mini Statement, Cash Deposit, Cash Withdrawal, remittances that are intra-bank or interbank in nature, on real time payment channel.
- b) To sub-serve the goal of Government of India (GoI) and Reserve Bank of India (RBI) in furthering Financial Inclusion.
- c) To sub-serve the goal of RBI in digitization of retail payments.
- d) To enable banks to route the Aadhaar and/or Virtual ID initiated interbank transactions through a central switching and clearing agency.
- e) To facilitate inter-operability across banks in a safe and secured manner.
- f) To build the foundation for a full range of Aadhaar enabled Banking services.
- g) eKYC Services¹
 - a. To enable a resident of India to open bank account with any bank, any location using Aadhaar as a Proof of Identity and Proof of Address.

¹ As of date 11th Feb'19, eKYC usage for account opening is only limited to receive DBT in the account. It may change in future, subject to further guidelines provided by UIDAI/amendment in Aadhaar act bill on time to time basis.

- b. To provide a real time electronic KYC platform to all banks in India which can help them in meeting their customer KYC needs.
 - c. To provide a cost effective, safe and secure means of paperless KYC to all banks in India which may save lot of cost and effort related to storing physical KYC proofs.
- h) To facilitate Aadhaar and/or Virtual ID based Merchant transactions by allowing the merchant to accept the Aadhaar and/or Virtual ID of the customer as a payment instrument for the purchase of goods and services through biometric authentication

3 Customers in AePS

Section 7 of the Aadhaar Act 2016 (Targeted Delivery of Financial and other Subsidies, Benefits and Services) outlines that welfare schemes funded from consolidated fund of India shall be availed using Authentication (AADHAAR shall be used as the mode of Authentication) in such a manner so as the benefits reach the deserving and is not siphoned away by middle men. Aadhaar can be linked to a bank account for use in carrying out banking transactions like, Balance enquiry, Mini statement, Cash deposit, Cash Withdrawal, Remittances, Purchase transaction and also for receiving of government entitlements like Direct Benefit Transfers, Social Security Pension or government subsidies etc. Any resident having his/her Aadhaar number linked to bank account can participate in AePS. Customer can participate in AePS through below channels

- a) The Customer access points may have Business Correspondents (BC) using Micro-ATM devices to facilitate customers to make Cash Deposit, Cash Withdrawal, Fund Transfer and Balance Enquiry and/ merchant facilitating purchase, refund transaction of BHIM Aadhaar Pay. The devices used by BC/Merchants should adhere to the standards as specified in the document on Micro-ATM standards.
- b) A Business Correspondent is an intermediary used by a bank to extend Banking services in areas where they do not have a branch. The scope of activities undertaken by the Business Correspondents includes, inter alia, collection of small value deposits, Cash withdrawals and small value interbank remittances. Member banks are advised to refer to various RBI notifications on Financial Inclusion from time to time for more details.
- c) Within the scope of AePS, a BC of a bank is treated as an integral part of the Bank that it corresponds with. The Bank will be known as Acquirer Bank. The Bank will be responsible for all acts of commissions and omissions of its BC.
- d) The customer access points can also be a biometric enabled ATM which has the capability to accept Aadhaar number from a card swipe or other means like manual entry or Virtual ID's manual entry and accept fingerprint/IRIS on a biometric scanner attached to microATM.

- e) A merchant POS terminal capable of accepting biometrics of the customer as a means of customer authentication can also be a customer access point.
- f) The Customer access points may have Business Correspondents (BC) using Micro-ATM devices to facilitate customers to make Cash Deposit, Cash Withdrawal, Fund Transfer and Balance Enquiry and/ merchant facilitating purchase, refund transaction of BHIM Aadhaar Pay. The devices used by BC/Merchants should adhere to the standards as specified in the document on Micro-ATM standards.

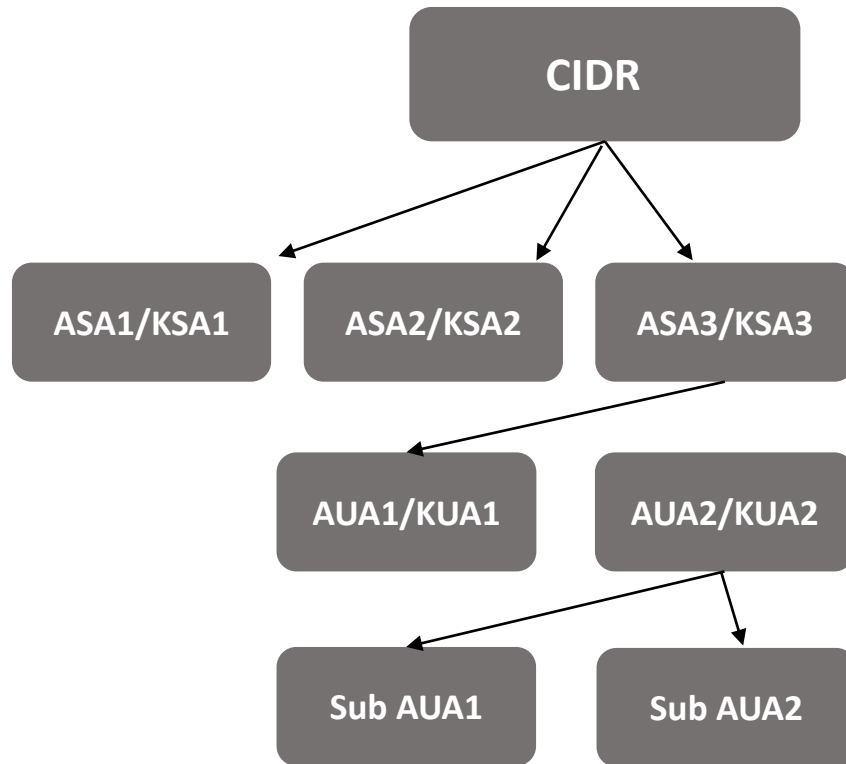
For all transactions whether intra-bank or interbank, a Transaction Receipt shall be printed and handed over to a customer as a transaction record with its finality status, by the BC/merchant through whom the transaction was initiated. The details provided in a transaction Receipt shall be as per the AePS Interface Specifications

In case of BHIM Aadhaar Pay transaction, printed receipt is optional, however e-receipt to customer should be provided [for the cases where physical receipt is not provided] by the acquirer bank & a notification for the debit transaction should go to customer from issuer bank as well as a result of successful transaction. Similarly, refund transactions should result in an e-receipt indicating credit.

4 Authentication operating Model

UIDAI engages with Authentication User Agencies (AUAs - who would deliver services to their beneficiaries by using Aadhaar based model for verification) and Authentication Service Agencies (ASAs). Below table explains in detail about AUA/ASA and other important actors in Aadhaar Authentication eco system.

NPCI in its capacity shall act as ASA aggregating various AUA for utilization of Authentication facility from UIDAI. A resident who Aadhaar number is linked to his/her Bank account approaches a delivery point (CSC, Business Correspondent etc) enabled with biometric enabled authentication device. Authentication devices shall collect Aadhaar number and biometrics and/or OTP, demographics of the resident for authentication purpose. AUA shall process the request in accordance with the specifications defined by its ASA and UIDAI. ASA shall receive the transaction from AUA and shall forward the same to CIDR (UIDAI data base) for verification of resident identity. ASA shall receive response for the subsequent request by resident which shall be forwarded to the respective AUA for necessary business action at their end.



Entity	Services Offered
CIDR	<ul style="list-style-type: none"> ✓ eKYC ✓ Auth ✓ OTP
ASA	<ul style="list-style-type: none"> ✓ Aggregator for above services from AUAs/ KUAs ✓ Connectivity with CIDR
AUA/KUA	<ul style="list-style-type: none"> ✓ Requesting Entity for Authentication services ✓ Services based on authentication to end consumer

An AUA can appoint Sub-AUAs who are not able to meet the UIDAI criteria for AUA license and hence add to an extra layer in authentication ecosystem. Sub-AUAs shall be provided a sub-AUA code which shall be used to identify the Sub-AUA in the ecosystem. A Sub-AUA can only perform authentication transactions using AUA license key and no eKYC transactions shall be allowed for Sub-AUAs.

	Development	Pre-Production	Production
Pre-requisite to access	No prerequisites- All prospective AUA can access	<ul style="list-style-type: none"> ✓ UIDAI-AUA agreement 	<ul style="list-style-type: none"> ✓ UIDAI checklist Go-live

UIDAI environments	the UIDAI development environment	<ul style="list-style-type: none"> ✓ Established connectivity with an UIDAI approved ASA 	<ul style="list-style-type: none"> ✓ Supporting documents
Pre-requisite at NPCI side	NA	<ul style="list-style-type: none"> ✓ Agreement with NPCI/ onboarding documentation ✓ Duly filled requirement template ✓ Pre-Production License keys from UIDAI 	<ul style="list-style-type: none"> ✓ Successful competition of certification ✓ Issuance of production license key from UIDAI ✓ Completion of all onboarding formalities at NPCI side as applicable

All AUAs are mandated by UIDAI to conduct audit of their operations and systems by recognized information system auditor before Go-live and the report has to be duly submitted to UIDAI. The following documents should be referred for compliance purpose

1. Aadhaar Authentication Standards and Specifications
2. UIDAI-AUA agreement

5 Membership

Pre-requisite to avail the membership of AePS, BHIM Aadhaar Pay & eKYC services is entity should have Authentication User Agency (AUA for Authentication services) & KYC User Agency (KUA for eKYC) agreements. Further, banks are also required to execute agreement and complete documentation for usage of AEPS services with NPCI.

All member banks shall strictly comply with the RBI's notifications on financial inclusion business correspondent guidelines, RBI notifications or circular on KYC/AML or PML/CFT guidelines or RBI notifications on use of eKYC service of UIDAI from time to time.

Note: The Regulatory Guidelines of Reserve Bank of India shall have over-riding effect over the provisions made in these Guidelines.

5.1 Terms of membership

1. Member bank has to be duly approved by UIDAI to use authentication services.
2. Have necessary documentation in place with UIDAI & NPCI for use of authentication services. & Bank should meet the below criteria
 - a. The applicant bank is a "Type A" member of the RBI's Real Time Gross Settlement System.

- b. The applicant bank is willing to contribute to Settlement Guarantee Fund of NPCI.
3. AePS Sub-membership model can be availed
 - a. Banks who have AUA license but not RTGS membership
 - b. Banks who don't have AUA license but should be sub-AUA of an AUA who is live with and/or not have RTGS membership

5.2 Certification

On admission of a bank as a member to participate in AePS and/or eKYC Service, NPCI will prepare a project plan detailing steps required for onboarding the entity on to AePS services. The interface specifications would be made available to bank upon approval of the application and admission of the bank in AePS and/or eKYC Service. Bank shall raise a formal request with NPCI for certification; NPCI shall allot a certification slot to entity on request once the application is developed. Certification shall be conducted based on a pre-defined test plan. Test script shall be released by NPCI post successful certification.

Terms & Conditions of Certification

1. Certification can be availed by entities at a pre-defined cost which shall be liable to change on a periodic basis. NPCI reserves right to amend/change certification fees on periodic basis, NPCI shall communicate the same to member entities.
2. If NPCI / UIDAI releases any new specification, NPCI reserves the right to upgrade the existing system. NPCI will examine if there is a need to re-certify either on account of bank/ NPCI related development changes.
3. If a member bank changes/added new switch for AePS services then member bank should notify NPCI and should allow NPCI to perform re-certification. All cost associated with re-certification will be borne by the member-bank migrating to new platform.
4. Member entity should take necessary measures at their end to ensure certification is completed as per the test plan shared by NPCI.
5. The certification shall be valid for a period of 90 days only. Post expiry of certification, member/ requesting entity has to perform recertification.

5.3 Member Notifications

NPCI shall notify all the member banks regarding:

- a) Revision of interchange and/or switching fee or any other commercials related to AePS membership
- b) Recovery of manual or exception charges arising out of membership in AePS
- c) Inclusion of a new member participating in AePS.
- d) Cessation of membership of any bank.

- e) Suspension/Termination of any member bank.
- f) Amendments in the AePS and eKYC Service Procedural Guidelines.
- g) New enhancement of the software and hardware released pertaining to the AePS or eKYC Service.
- h) Changes in the periodic maintenance hours.
- i) Any other issues deemed important by NPCI for the member banks.

5.4 Termination of services

NPCI under the following circumstances may terminate/suspend the AePS and/or eKYC Service membership:

- a. The member has failed to comply with or violated any of the provisions of the AePS and/or eKYC Service Procedural guidelines, as amended from time-to-time.
- b. Member commits a material breach of AePS and/or eKYC Service Operating Procedures, which remains un-remedied for thirty (30) days after giving notice.
- c. The current account with RBI of the member bank is closed or frozen or cancelled
- d. The member bank is amalgamated or merged with another member bank.
- e. Steps have been initiated for winding up the business of the member bank.
- f. Any regulators' instructions will lead to termination of services of entities.

Process of AePS Membership's Termination/Suspension

- a) NPCI shall inform in writing to the member bank regarding termination/suspension of its membership to AePS and/or eKYC Service.
- b) If NPCI is of the opinion that the breach is not curable, it may suspend/terminate the AePS and/or eKYC Service membership with immediate effect. However, the member bank shall be given an opportunity to be heard within thirty (30) days and confirming or revoking the termination/suspension passed on earlier.
- c) NPCI may at any time, if it is satisfied, either on its own motion or on the representation of the member that the order of suspension/termination of its membership may be revoked, it may pass on accordingly.

- d) If the breach is capable of remedy but cannot be reasonably cured within thirty (30) days period, termination/suspension will not be effective if the member in default commences cure of the breach within thirty (30) days and thereafter diligently peruses such cure to the completion within sixty (60) days of such notice of breach.
- e) The member bank whose termination of membership has been revoked shall be entitled to apply for membership afresh in accordance with AePS Procedural guidelines.

NPCI reserves the right to impose a fine on member banks participating in the AePS and/or eKYC Service upon violating the Operating Settlement Guidelines for AePS and/or eKYC Service. In the event of non-compliance with the Operating Settlement Guidelines -AePS and/or eKYC Service, NPCI reserves the right either to notify the member bank or shall directly impose penalty on the member bank depending on its past record. No fines shall be imposed, if the rectification is done within the stipulated time frame, as set by NPCI, failing to abide by shall be subject to steering committee recommendations/legal penalties. Fines will be billed separately and shall be sent to the respective member banks. It is obligatory on the part of all member banks to clear all pending dues i.e. fines, etc. within the stipulated time frame as set by NPCI, failure to comply with, shall result in suspension/termination from further participation.

6 Products & Services

Aadhaar Enabled Payment System (AePS) is a bank led model which allows online financial inclusion transaction at Micro-ATM/Kiosk/mobile through the Business correspondent of any bank using the Aadhaar authentication. This system is designed to handle both ONUS and OFFUS requests seamlessly in an effective way by enabling authentication gateway for all Aadhaar linked account holders. The services offered:

Services Offered	Transaction type (ONUS/OFFUS)
1. Bio Metric & OTP based Authentication / ONUS transactions	1. Balance Enquiry
2. OFFUS transactions	2. Cash Withdrawal
3. Best Finger Detection (BFD)	3. Cash Deposit
4. eKYC	4. Aadhaar to Aadhaar Fund Transfer
5. Demographic Authentication	5. Mini Statement
6. Tokenization	6. BHIM Aadhaar Pay
7. Aadhaar Seeding status through Micro ATM	7. Refund transaction* ²
	8. SHG Transaction* ³

² This is yet to be introduced as on 11th Feb'19

³ This is yet to be introduced as on 11th Feb'19

All services mentioned above may be collectively referred to as AePS group of services.

6.1 Aadhaar Authentication/ ONUS

In case of ONUS transactions, Acquirer and Issuer banks will be the same. In any Aadhaar enabled financial transaction, whether intra-bank, a customer is required to provide his Aadhaar number and/or Virtual ID and biometrics on the Micro-ATM managed by a BC to prove his/her identity and get himself/herself authenticated by the UIDAI. A transaction will be sent to acquiring bank only when the Aadhaar authentication is successful. Micro-ATM/kiosk/mobile device that submits Aadhaar/Virtual ID and the biometrics to UIDAI should adhere to the 'Aadhaar Authentication API and Devices Security Specification and Biometric Fingerprint Scanner Specifications' of the Unique Identification Authority of India for Aadhaar authentication referred to in latest NPCI specification document. A positive Aadhaar authentication is an indispensable part of any Aadhaar enabled financial transaction.

NPCI facilitates Aadhaar authentication service too. Banks, therefore, have an option to route their intra-bank transactions to NPCI switch for Aadhaar Gateway Authentication.

6.2 Aadhaar enabled interbank (Off-us) Transactions

In case of AePS OFFUS transactions, acquirer bank and issuer bank will be different banks. Transaction request will be initiated from acquirer bank's terminal and issuer bank will get pre-approved request from the NPCI as the customer's Aadhaar/VID has been authenticated with UIDAI's CIDR. In case of OFFUS transactions, customer has to provide Aadhaar number/Virtual ID, Issuer bank name (IIN), Type of transaction, Value (if financial transactions) & bio-metric.

The Aadhaar enabled basic types transactions are as follows. These transactions type are available on AePS ONUS & OFFUS both. Member banks live on AePS OFFUS as an Acquirer has to mandatorily provide all services under AePS to the end customer service points as mentioned below.

- a) Balance Enquiry
- b) Cash Withdrawal
- c) Cash Deposit
- d) Fund transfer
- e) Mini Statement
- f) SHG Dual Authentication Transactions⁴

6.2.1 Balance Enquiry

Balance Enquiry is a non-financial transaction. If it is On-Us, the bank upon a successful Aadhaar/Virtual ID Authentication, advises the balance in the customer's AEBA to the Micro-ATM that originated the Enquiry. If it is off-us, upon successful Aadhaar/Virtual ID Authentication, the Balance advice received from the Issuer bank will be forwarded to Micro-ATM/kiosk that originated the Enquiry, through NPCI and acquirer switches.

⁴ This is yet to be introduced as on 11th Feb'19

6.2.2 Cash Withdrawal

A Bank customer would make a Cash withdrawal through the Micro-ATM of a bank operated by a BC/CSP or even at a biometric enabled ATM. The cash withdrawal transaction first flows to the acquirer bank. If the transaction is ONUS in nature, on successful Aadhaar Authentication, the bank will debit the customer's account and send its positive response to the Micro-ATM. If it is OFFUS in nature, on successful Aadhaar Authentication, the Issuer Bank will debit the Aadhaar enabled account of the customer and send its positive response to the acquirer via NPCI switch; acquirer will finally send it to MicroATM/ATM. Whether ONUS or OFFUS, only after receipt of a positive response, cash will be dispensed.

If the response from the Issuer bank is not received within a set time limit, the issuer bank will receive reversal notification from NPCI switch or the Acquirer Bank depending upon who got the response timed-out. No money will be dispensed to the initiating customer by BC.

A cash withdrawal is possible from the initiating customer's own Aadhaar enabled account only. Operating and Settlement Guidelines shows the transaction flow in respect OFFUS cash withdrawal transactions.

6.2.3 Cash Deposit

A Bank Customer would make a Cash Deposit through a BC who uses a Micro-ATM terminal. A cash deposit transaction flows to the acquirer bank of the BC. If the transaction is ONUS in nature, on successful Aadhaar Authentication, the bank will credit the customer's account and send a positive response to the Micro-ATM. If it is OFFUS in nature, on successful Aadhaar Authentication & beneficiary account validation; cash will be captured by BC and a receipt will be generated. Then the Issuer bank will credit the customer's Aadhaar enabled account and send its response through NPCI and acquirer switches, for having credited the account.

A cash deposit is possible for credit to the initiate customer's own Aadhaar enabled account only. Operating and Settlement Guidelines shows the transaction flow in respect OFFUS cash deposit transactions.

6.2.4 Aadhaar to Aadhaar Funds Transfer

In AePS, an Aadhaar/Virtual ID to Aadhaar funds transfer, remitting customer should necessarily have his/her Aadhaar enabled Account with the Remitting Bank and the transfer will be effected only after a successful debit to this account. A Remitting Customer is required to initiate an Aadhaar enabled OFFUS in nature remittance only from the Micro-ATM of a Bank with whom he/ she is holding an Aadhaar enabled Account.

When a Funds Transfer transaction is initiated from a Micro-ATM of a BC, the Remitting Bank firstly, gets the transaction Aadhaar/Virtual ID authenticated. Upon successful Aadhaar/Virtual ID Authentication, the bank debits the Aadhaar enabled account of the initiating customer with the remittance amount and sends a Payment Request to the Beneficiary's Bank based on the IIN provided, through the NPCI Switch. Beneficiary's Bank would credit the Beneficiary's Aadhaar enabled account and forward its positive

response to the Micro-ATM that initiated the request, through NPCI switch. The customer will know the finality of the remittance from the Transaction Receipt.

If the response from the beneficiary's bank is not received within a set time limit, no reversal notification from NPCI switch or the Acquirer Bank or the Micro-ATM will be sent to the beneficiary's Bank. For all interbank remittances that have got timed out, Banks are advised to use the Dispute Management System referred to herein to resolve interbank settlement issues.

Fund Transfer is possible only from one Aadhaar Enabled account to another Aadhaar enabled Account. Operating and Settlement Guidelines shows the transaction flow of Aadhaar to Aadhaar Fund Transfer and different settlement exception cases.

In any typical funds transfer, there would be six parties:

- i. Customer having it Aadhaar linked to account
- ii. Remitting Bank's switch (plus Business Correspondent Agent)
- iii. NPCI - AePS Switch
- iv. UIDAI
- v. Beneficiary Bank's Switch
- vi. A Beneficiary with Aadhaar Enabled Bank account

6.2.5 Mini statement

Mini Statement is a non-financial transaction which will help a customer track his previous transactions. A Mini statement may be on-us or off-us. If it is On-Us, the bank upon a successful Aadhaar Authentication, advises the previous transactions (maximum 10) and balance in the customer's account to the Micro-ATM that originated the enquiry. If it is off-us, a Mini statement request will be forwarded to the issuer Bank through NPCI. Upon successful Aadhaar Authentication, the previous transactions (maximum 10) and balance advice received from the Issuer bank will be forwarded to Micro-ATM that originated the Enquiry, through NPCI switch.

6.2.6 SHG Dual Authentication Transactions⁵

A self-help group is financial intermediary committee usually composed of 10–20 local women or men. SHG promotes the small savings within the group. The savings are being kept with the banks. SHG usually have 2-3 leaders & these leaders are allowed to perform the financial transactions with banks on behalf of group. Transactions being performed are Cash Withdrawal, Cash Deposit from SHG's account and Fund Transfer from SHG's bank account to individual's bank account. To facilitate the goal of financial inclusion, SHG transactions can be performed through AePS channel. For that Leaders' of SHG Aadhaar authentication will be performed and post successful authentication transactions will be carried out. All stakeholders have to comply with SHG guidelines provided by sector regulators on time to time basis.

⁵ This is yet to be implemented

6.3 BHIM Aadhaar Pay

BHIM Aadhaar Pay service is built atop AePS platform, as an additional transaction type, which allows a customer to perform a purchase transaction with a participating merchant channel using his/her Aadhaar linked bank account and biometric. BHIM Aadhaar Pay Common Application has two component: (i) Merchant Onboarding (ii) Payment/purchase Transaction

Merchant Onboarding will allow merchant to apply to an acquirer bank of his choice from a pre-approved list of banks for participating in this scheme, which will allow accepting payment through BHIM Aadhaar Pay for the sale of goods & services to the customer with Aadhaar Enabled Bank Account (AEBA).

Purchase Transactions

This functionality will allow the customer to perform a purchase transaction using his Aadhaar number/Virtual ID and biometric (Fingerprint/IRIS), the transaction will be ONUS/OFFUS in nature allowing any bank customer to transact on the Aadhaar based Merchant application of any bank.

A Bank customer would make a payment transaction through the merchant based mobile application/Kiosk/Micro-ATM with certified or any form factor along with the STQC standards.

The merchant pay transaction first flows to the Acquirer Bank of the merchant. If the transaction is ONUS in nature, on successful Aadhaar/Virtual ID Authentication, the bank will debit the customer's account and send its positive response to the mobile application. If transaction is OFFUS in nature, the transaction will be forwarded to the Issuer Bank through NPCI's switch. On successful Aadhaar/Virtual ID Authentication, the Issuer Bank will debit the Aadhaar enabled account of the customer and send its positive response to the mobile application of the merchant through the NPCI switch. Whether intra-bank or interbank, sale of goods and services should happen only after receipt of a positive response.

If the response from the Issuer bank is not received within a set time limit, the issuer bank will receive reversal notification from NPCI switch or the Acquirer Bank depending upon who got the response timed-out. No goods and services will be provided to the initiating customer by Merchant. Merchant Disputes and Settlement will be handled by Corresponding Acquirer Banks.

Refund transaction⁶

In case, customer wish to return the purchased good, refund transaction can be requested by customer at merchant point. Merchant must authorize such refund transactions, funds would be debited from merchant account to the customer account which participated in the original transactions. This facility may be available for the transaction performed during a defined period, as guided by the AePS Steering Committee.

⁶ This is yet to be introduced as on 11th Feb'19

6.4 Best Finger Detection

Best Finger Detection Identifies the best finger for a resident is the one that, when selected for authentication, provides the highest chance of successful authentication for that customer.

The best finger to be used for authentication depends on the intrinsic qualities of the finger (ex. ridge formation, how worn out they are, cracked, etc.), as well as the quality of images captured during enrolment process and the authentication transaction.

BFD application requires a customer to provide biometric authentication through each of the ten fingers one-by-one. All ten fingerprints along with the Aadhaar number are sent to UIDAI, which in turn returns a response indicating which fingers are best suited for Aadhaar biometric authentication.

6.5 eKYC transaction

A customer willing to open an account with a bank or perform re-KYC can avail benefit of *eKYC Service*, if he/she carries a valid 12 digit Aadhaar number or 16 digits Virtual ID. Banks are required to have biometric scanners, complying with UIDAI standards, at branch or BC outlet. They are also required to have a client application to take customer Aadhaar number and fingerprint as input.

For using *eKYC Service*, bank may ask customer to provide his/her Aadhaar number/Virtual ID and fingerprint to do real time KYC. Bank must ensure to have customer consent before initiating such transaction. The transaction from the terminal will be transmitted to UIDAI by NPCI via bank server and then UIDAI will do further processing at their end. After the successful matching of Aadhaar number/Virtual ID and fingerprint, UIDAI will provide relevant information present at their end in conjunction to the information sought in request. Bank may choose to save customer demographic details in a manner prescribed by UIDAI, and, security of such data must be maintained at all times.

6.6 Demographic Authentication

Aadhaar authentication supports authentication using multiple factors. These factors include demographic data, biometric data, OTP, or combinations thereof. Adding multiple factors increases the strength of authentication. Applications using Aadhaar authentication through demographic details is known as Demographic Authentication.

Demographic authentication service provides services to instantly verify the identity of the Aadhaar holder against the available data in UIDAI. Based on the needs of the service, different identifiers could be used along with Aadhaar Number. These identifiers could be combination demographic information such as identify /Address (Name, Date of birth, Address). 100% match of these data fields (which is being sent by requesting entity against the data in CIDR) has been mandated by UIDAI for the demographic authentication.

Bank must ensure to have customer consent before initiating such transaction. The transaction from the terminal/Banks switch will be transmitted to UIDAI by NPCI and then UIDAI will do further processing at their end. After the successful matching of Aadhaar number and demographic details, UIDAI will provide a success/failure response.

7 Roles & Obligation of members

7.1 Acquirer Bank shall be responsible for the following:

- i. Aadhaar Number/Virtual ID logic verifications. (verhoeff algorithm)
- ii. Limits on the Transaction amount, if any
- iii. Debit BC account before initiating Cash Deposit transaction request
- iv. Compliance of Business Correspondence w.r.t. BC/CSP Agent should not charge customers for AePS set of transactions. Proactively curbing the unethical practices in order to prevent potential fraudulent transactions.
- v. There should not be any sub-limits set on the transactions amount in AePS at Acquirer/Corporate BC/BC/CSP end. If found otherwise, will invite penalty on Acquirer Bank.
- vi. Penalty will be levied on Acquirer failing to take action for control measures on the Round Tripping & Split transactions.
- vii. Any fraudulent transactions originated from BC/CSP Agent will be the responsibility of acquirer bank.
- viii. Initiating multiple requests from same Micro-ATM within the transaction time period with same reference/transaction number (This is to avoid responding to multiple requests for one and the same transaction)
- ix. Daily Reconciliation to be performed and necessary actions to be taken as per the latest operating and settlement guidelines to facilitate the customers.
- x. Adequacy of Collateral posted with NPCI towards NDC compliance.
- xi. Adequacy of contribution to Settlement Guarantee Funds
- xii. AML related validations for Funds Transfer transaction for the debit leg (online or offline)
- xiii. Fraud Check (online or offline) & reporting
- xiv. All acts of commissions and omissions of the Bank's BC/CSP agents.
- xv. Compliance to UIDAI eKYC API, Auth API, BFD API, OTP API depending upon the type of service availed.
- xvi. Compliance to all transaction security and hardware standards mandated by UIDAI.
- xvii. Comply with NPCI's AePS Procedural Guidelines & Operating and Settlement guidelines.
- xviii. Comply to the guidelines issued by RBI, UIDAI on time to time basis
- xix. Strict Adherence to latest AePS specification issued by NPCI on time to time basis.
- xx. Onboarding of BC/CSP agent should only be done post checking compliance with BC registry.⁷

⁷ This will be applicable once BC registry gets operationalized.

- xxi. Acquirer bank is liable for the third party service providers[i.e. Application Service Providers, Corporate BCs] which they involve for the AePS set of products. Acquirer banks have to ensure that these third party service providers abide the procedural guidelines of AePS, circulars of NPCI, guidelines issued by regulators on time to time basis.
- xxii. Acquirer bank needs to adhere to the branding guidelines of the product.

7.2 Issuer Bank shall be responsible for the following

- i. Issuer Aadhaar/Virtual ID Authentication and posting of transaction to an Aadhaar enabled Account in respect of Cash Deposit, Cash Withdrawal and other financial transactions.
- ii. Posting of transaction to the beneficiary's account in respect of interbank funds transfer between two Aadhaar enabled accounts.
- iii. Checks on Multiple Requests for one and same Aadhaar related transactions types for a transaction with same ref/transaction number (This is to avoid responding to multiple requests for a single Payment Request)
- iv. Maximum permissible limit in a day, if any.
- v. AML related validations for Funds Transfer transaction for credit leg (online or offline).
- vi. Fraud Check (online or offline) & reporting.
- vii. Strict Adherence to latest AePS specification issued by NPCI on time to time basis.
- viii. Daily Reconciliation needs to be carried out and necessary actions to be taken post reconciliation.
- ix. Compliance to NPCI's AePS Procedural Guidelines & operating and settlement guidelines.
- x. Compliance to the guidelines issued by RBI, UIDAI on time to time basis.
- xi. Correct Aadhaar seeding/linking with customer's account is the responsibility of issuer bank.
- xii. Issuer bank is liable for all the third party service providers[i.e. Application Service Providers, Corporate BCs] which they involve for the AePS set of products. Issuer banks have to ensure that these third party service providers abide the procedural guidelines of AePS, circulars of NPCI, guidelines issued by regulators on time to time basis.
- xiii. Issuer side transaction level limits needs to be implemented for offus financial transactions.
- xiv. Issuer bank needs to adhere to the branding guidelines of the product.
- xv. Issuer bank needs to adhere to standardize AePS narration in passbook entries, to be followed as per proposed format prescribed and agreed by Steering committee
- xvi. Mandatory SMS is need to be sent to customers for AePS financial transactions by issuer bank for each debit entry in customer's account through AePS/BHIM Aadhaar channel.

8 AePS Steering Committee

The Steering Committee to be called as the AePS Steering Committee, is formed to take key decisions with respect to AePS product on behalf of the AePS ecosystem member banks. It would also have the mandate to come out with policy level suggestions and product level enhancements and features wherever and whenever required and impose regulations and rules along with disincentives towards enabling best practices in product governance and compliance.

8.1 Composition of Steering Committee

1. The AePS Steering Committee will comprise of Banks which come under the 2nd Schedule of the Reserve Bank of India.
2. The composition of the Banks would be a good representation of Public Sector Banks, Private Banks, Regional Rural Banks, Payment Banks, Small Finance Banks, and Cooperative Banks.
3. The Steering Committee will have the authority to evaluate new entrants to Steering Committee and also to remove existing members.
4. The Steering Committee reserves the right to invite member banks who are not part of the steering committee as Special Invitees. Such Special Invitee Banks should not exceed more than 2 in numbers per each Steering Committee Meeting.
5. An exception to the number of special invitee banks may be taken under specific circumstances subject to prior approval of the majority of the Steering Committee Members.
6. The regulatory bodies like RBI, IBA or NABARD can also be part of the Special Invitee and such invitations will not need the prior approval of the SCM
7. The UIDAI being the integral part of the AePS product will be the permanent Special Invitee for all SCMs.
8. The NPCI reserves the right to appoint or nominate participation from AePS department and other internal departments from time to time and as needed or deemed fit.

8.2 Functions of Steering Committee

1. The Steering Committee will have the authority to define rules and disincentives for product compliance as per the AePS Procedural guidelines and impose, monitor regulatory compliance.
2. The Steering committee will have the authority to define, implement, regulate and monitor the various charges in the AePS ecosystem which includes the Interchange structure, and in a limited capacity to recommend the switching fees and various commission structures in the AePS value chain.
3. The SCM may decide to form Working Groups, User Groups, or Sub Committees comprising of both SCM, and/or, non-SCM Banks or entities for taking decisions over special matters as and when required. The formation, tenure, terms of reference, expected outcome and dissolving of such groups will be decided by the SCM.

8.3 Nomination and Terms of office

1. The Chair of the Committee would be the Product Head of AePS at NPCI, however in scenarios where other senior officials from NPCI like SVPs, CTOs, COOs, CEOs or CXOs are present, the Senior most Official will be the Chair of the Committee, also where ever the Product Head of AePS is not present, the next senior level official from NPCI present in the meeting will be the designated Chair.
2. The Member Banks will be required to nominate officials not less than the designation of GM and above for Public Sector Banks and GM and equivalent for Private Sector and other Banks, such nominations would be reviewed each year by way of formal letters to be sent by each Member Bank addressed to the Head of Department, AEPS, NPCI.
3. Wherein a Member Bank desires to nominate officials over and above the GM level designate, such nomination should be limited to One Official, thus the sum total of nominations per member bank should not exceed 2 in number.
4. In case the nominated officials not being able to attend the SCM, the same would be treated as absence from the SCM and no other officials other than the nominated officials would be invited to attend.
5. In the event that a nominated official resigns during their term of office, s/he will automatically be replaced by the alternate, and a new alternate will be determined by way of filing a fresh nomination to NPCI.
6. The list of the final nominated officials is to be shared with all the member banks by NPCI

8.4 Frequency of meetings & Quorum

1. The SCMs will be held once a quarter every financial year. Further, under special circumstances the SCM can be called for at any time of the year. In such cases it would be treated as over and above the 4 SCMs per year and accordingly numbered and recorded.
2. The Sub Committees or User Groups or Working groups will meet as per the business requirements to arrive at the expected outcome.
3. For all SCMs, a quorum is a majority of members of the committee, excluding vacancies.
4. Some committees may, in addition, require a minimum number of attendees of a particular category, for example, a representative from each member bank. The minimum number for SCMs is 50% of issuers and 50% of acquirers of Steering Committee issuers and acquirer.
5. Should a quorum not be present at the start of the meeting the Chair may, with the consent of those present, proceed with the meeting on the understanding that any decisions reached will be subject to
 - a. Approval provided on mail to the draft minutes by the absentee banks or

- b. Ratification when a quorum is present, or at the next meeting at which a quorum is present, or by round robin.

8.5 Decision making

1. Decision making is based on the principle of sufficient consensus.

8.6 Functions of members

1. Members are expected to conduct themselves in accordance with the guidelines of the AePS Steering Committee.
2. Members must share with NPCI the nomination letter for AePS SCM annually on the bank's letter head duly signed by not less than the GM or equivalent.
3. Members must share with NPCI the nomination letter for AePS SCM annually on the bank's letter head duly signed by not less than the GM or equivalent.
4. Members are expected to participate actively in the deliberations of the committee.

8.7 Functions of Chair

1. The Chair shall conduct the meeting with the appropriate degree of formality.
2. The role of the Chair is to manage consensus.
3. At the end of each item, the Chair shall summarize what has been agreed, the wording of any resolutions and decisions taken, and who is responsible for any actions required, to ensure that all are in agreement.

The Chair shall review the draft minutes and return them, with amendments as appropriate which shall then be circulated to the members.

9 Governance of AePS ecosystem

9.1 AePS group of Services Availability

All AePS group of Services except Demo Auth and tokenization(as it is not customer facing) shall be in operation/ available to all member banks on 24 x 7 basis with 99.5% uptime except in the event of force majeure such as war and natural calamities and a regular periodic maintenance with prior notice. However, the regular periodic maintenance of the NPCI systems shall be notified to all member banks 36 hours in advance.

9.2 Audit by NPCI

NPCI reserves the right to audit the AEPS related systems (including Hardware and software) of the member banks or their Business Correspondents if found necessary.

9.3 NPCI ASA liability

NPCI as ASA is aggregating the authentication requests for the AePS group of services and the final authentication is done by UIDAI alone. Thus, NPCI shall have no liability arising out of successful transaction due to “False Accept” by UIDAI.

The owner and co-coordinator of AEPS group of services is NPCI. NPCI reserves the right either operate & maintain the AEPS and eKYC Service and the Network on its own or obtain necessary services from third party service providers.

9.4 Non-Disclosure Agreement

All members participating in the AePS Network should sign a non-disclosure agreement with NPCI as given in Annexure-V. Each member should treat AEPS related documents as strictly confidential and should not disclose to alien parties without prior written permission from NPCI, failing to comply with, shall invite severe penalties. However, the participating members can disclose the AEPS Procedural Guidelines within its employees or agents related to the specific areas.

9.5 Indemnification

It is binding on all members, including NPCI, participating in *AePS and e-KYC* to defend and indemnify themselves from all loss and liabilities if any, arising out of the following:

- a) Member’s failure to perform its duties and responsibilities as per the Procedural guidelines for *AePS, eKYC Service and as prescribed by domain regulator.*
- b) Malfunctioning of Member’s equipment.
- c) Fraud or negligence on the part of member.
- d) Unauthorized access to *AePS* and/or *eKYC Service* Network.
- e) Member’s software, hardware or any other equipment violating copyright, patent laws and UIDAI authentication policy etc.

All members should comply with the *AePS* and *eKYC Service* Procedural Guidelines as framed by NPCI. NPCI reserves the right to impose penalty on the members either by suspending or terminating (Host-to-Host) connectivity for violations of the *AePS* and *eKYC Service* Procedural Guidelines.

9.6 Prohibition to Use NPCI Logo/ Trademark /Network

Upon termination from *AePS* and/or *eKYC Service*, the bank shall abstain from further using the *AePS* and/or *eKYC Service* Trademark with immediate effect and failure to comply with the same, shall invite legal proceedings.

Banks that have been terminated from AePS and/or eKYC Service membership shall be deprived of the privilege to use NPCI Switch for any transactions.

Any pending dispute pertaining to transaction errors not resolved before the member bank is terminated will be retrieved from the respective bank's settlement account.

The terminated member bank shall not disclose any information regarding the AePS and/or eKYC Service Network or any knowledge gained through participation in the AePS and/or eKYC Service Network to the external world. Failure to comply with the same shall be treated as breach of trust and will invite legal penalties. This rule shall be binding on the terminated member bank for One (1) year from the date of the termination.

9.7 Penalty or Fine

NPCI reserves the right to impose a fine on member banks participating in the AePS and/or eKYC Service upon violating the Operating Settlement Guidelines for AePS and/or eKYC Service.

9.8 Deviation from AePS and/or eKYC Service Operating Procedures

In the event of non-compliance with the Operating Procedures-AePS and/or eKYC Service, NPCI reserves the right either to notify the member bank or shall directly impose penalty on the member bank depending on its past record. No fines shall be imposed, if the rectification is done within the stipulated time frame, as set by NPCI, failing to abide by shall be subject to steering committee recommendations/legal penalties.

9.9 Pending Dues

It is obligatory on the part of all member banks to clear all pending dues i.e. fines, etc. within the stipulated time frame as set by NPCI, failure to comply with, shall result in suspension/termination from further participation.

9.10 Invoicing

Fines will be billed separately and shall be sent to the respective member banks. The fines shall be payable to NPCI in accordance with the terms and conditions as defined in the invoice.

9.11 Compliance to Reserve Bank of India Guidelines

All member banks shall strictly comply with the RBI's notifications on financial inclusion business correspondent guidelines, RBI notifications or circular on KYC/AML or PML/CFT guidelines or RBI notifications on use of eKYC service of UIDAI from time to time.

The Regulatory Guidelines of Reserve Bank of India shall have over-riding effect over the provisions made in these Guidelines.

9.12 Amendment to the Procedural Guidelines

NPCI may issue amendments to these Guidelines from time to time by way of circulars. The revised versions of the Guidelines may also be issued incorporating the new provisions periodically.

9.13 KYC/ AML Compliance as per RBI guidelines

It would be the responsibility of the issuer/remitter banks to check any unusual pattern of remittance if any in respect of their respective customers. We have given in Annexure VI, a declaration to be signed and submitted to NPCI in this connection, by the member banks.

10 Components, Communication and Settlement

10.1 Interbank Settlements and Net Debit Cap (NDC)

All Aadhaar enabled interbank remittances result in interbank settlements. The interbank settlement for AePS takes place once a day on a netted basis. These transactions are simply referred to as interbank transactions for the purpose of convenience herein below:

- a) NPCI would compute a member bank's net position (payable or receivable) on successful execution of all its interbank transactions on a real time basis.
- b) The net position of a member bank so computed should always be within the "Net Debit Cap (NDC)" prescribed for that bank. Processing of outgoing transactions of a bank, when its net exposure exceeds its NDC during a day, would be stopped until NDC limit gets reset post transaction cut off.
- c) NDC fixed for Aadhaar enabled interbank transactions is exclusively for AEPS and no portion of it can be shared with NPCI's other services like NFS, IMPS, UPI, RuPay etc. and vice versa.
- d) Minimum Joining Fee / collateral would be Rs.5,00,000/- (Rupees five lakhs). The collaterals deposited with NPCI will be in form of non-interest bearing deposits. Banks Transactions would be reviewed periodically and accordingly bank will have to contribute additional collateral based on their transaction throughput.
- e) At the close of a AEPS business cycle on any day i.e., at 23.00 Hrs., the net receivable or payable in respect of each member bank, will be generated and a Daily settlement report for all Aadhaar enabled interbank transactions will be made available for download from the AEPS DMS solution[Data Navigator] to all member Banks. The Net Settlement Amount will be

inclusive of the Interchange, Transaction switching and settlement fees etc., payable by Member Banks.

f) NPCI's Type-D membership is activated and will arrange for the necessary inter-bank settlement of credits and debits to the banks' respective current accounts with RBI. .

g) The settlement time would usually be the first hour (09.00 hr.) of the next working day at RBI Mumbai, through RTGS. Please refer to paragraph 3.1.5, 3.1.6, 3.1.7 of the RBI notification referred to in Annexure-III.

h) It will be members' responsibility to verify the accuracy of the Daily Settlement Reports with reference to the data available at their end.

i) In case of net debit, a member bank has an obligation towards other member banks. Banks are therefore advised to ensure strict compliance to the RTGS operational instructions of RBI in this connection. Any failure to maintain the required balance in the RTGS settlement account shall attract penal action from RBI.

j) All banks before participating in AEPS shall issue a Letter of Authority to RBI authorizing them for AEPS related settlements in their respective accounts by NPCI or its settlement agency, duly approved by their respective boards. (Annexure-IV).

o) In this connection, Member Banks are required to be guided by paragraph 3.3 of the notification from the Department of Payments and Settlements of the Reserve Bank of India, Ref No: RBI/2010-11/218 DPSS.CO.CHD. No.695/03.01.03/2010-2011 dated 29th September, 2010 – (Annexure-III).

p) A bank failing to meet the clearing liability more than two times in a month or three times in a quarter would be debarred from AEPS membership.

10.2 Choice of Connectivity

Member Banks have to connect to AePS group of services directly from their own switch or through their technology Service Provider's Switch located at the bank's premises Or NPCI empanelled Application Service Provider hosted externally.

10.3 Message Formats

All AePS, BHIM Aadhaar Pay and eKYC Service transactions routed through the bank switch should comply with the message formats specified by NPCI as a part of AePS Interface specification and eKYC Service specification referred to in paragraph 1.b. hereof, with modifications if any communicated to member banks from time to time.

10.4 Transaction Logging

NPCI shall maintain logs of all Aadhaar/Virtual ID transactions passing through the NPCI switch. Member Banks are also advised to store transactions logs as per Aadhaar ACT/ regulation/ banks own policies whichever have longer duration.

10.5 Reports and Reconciliation

Following reports will be made available to the member banks:

- a) RAW data files
- b) Net Settlement report (NTSL) / Daily Settlement report (DSR)
- c) Verification files.
- d) Adjustment reports
- e) Payable / receivable (day wise & bank wise) service tax reports
- f) Invoice copy

Member banks shall ensure that they download these reports and keep their settlement accounts reconciled on a daily basis. Any loss arising due to not carrying out reconciliation on T+1 basis will be owned fully by the respective banks.

Besides these reports, Raw Transaction Data files, Settlement Files, Verification Files and Daily settlement Reports of all the Originating and responding transactions of a bank will also be available to the banks for download. In case of any discrepancy in the raw transaction data file, the reports cited above will be deemed as authentic.

10.6 AePS Dispute Management System and Exceptions handling

Disputed transactions are those that are reported as reconciled for a long time in the settlement accounts of the member banks or disputed by customers. NPCI has provided Dispute Management systems on similar lines as DMS[Data Navigator] for NFS to help member banks raise charge back/ re-presentments or make credit/debit adjustments to resolve all disputes arising out of Aadhaar enabled banking transactions.

Member banks shall collaboratively endeavor to settle discrepancies in Settlement, if raised by other member banks. Where necessary, NPCI shall provide transaction logs as logged by the SWITCH, if any, relating to the transaction reported as exception to facilitate settlement of the same.

Exception handling for onus transactions in case of authentication failure by UIDAI for absence of last mile connectivity (device) or extremely worn out biometrics of customers even after repeated attempts etc. banks need to put in place appropriate internal exception handling mechanisms in view of customer service

10.7 Customer Complaints- change as per AePS

Any complaint about customer account debited without cash being dispensed at BC or cash deposited/ debit made without corresponding credit to the beneficiary account should be conclusively and bilaterally dealt with by the remitting and beneficiary banks within 7 days from the date of receipt of a complaint

Annexure-I

(On the Letter Head of the Applicant Bank)

Date:

Application for AePS Membership

The Head of Department
AePS
National Payments Corporation of India
1001A, B wing 10th Floor,
The Capital, Bandra-Kurla Complex, Bandra (East),
Mumbai - 400 051

Dear Sir,

Subject: Aadhaar Enabled Payment System (AePS) Membership.

We would like to participate in the Aadhaar Enabled Payment System (AePS) and agree to the following items as under:

1. We have access to the UIDAI terms & Conditions for AUA/KUA as prescribed and have agreed to the Aadhaar Act 2016.
2. We agreed to deploy devices as per Micro ATM guidelines and STQC certified biometric devices and RBI guidelines.
3. Kindly take a note of details provided below:

Name of the Bank	
NFS Member	<input type="checkbox"/> Yes <input type="checkbox"/> No Since_____
Type of Membership	<input type="checkbox"/> Direct <input type="checkbox"/> Sub Member
Sponsor Bank Name	

Connectivity Option	Bank Switch/ASP Switch (Name of ASP)
Sharing of Switch	Is the Switch connectivity to NPCI is dedicated or shared with other banks?
Location of Switch	
AePS Contact Person Name (A Single Point of Contact)	
Telephone Number	
Fax Number	
Email ID:	
Brief Details: Hardware: Software: Network:	

Authorized signatory
(With sign and Stamp)

Date:

Annexure-II

BIN UPDATION FORM

(On Bank Letter Head)

Reference No.:

Date:

To,
The Head
AEPS
National Payments Corporation of India
Units Nos. 301, 302, 3rd Floor
Raheja Titanium, Western Express Highway
Goregaon (East), Mumbai - 400 063

Subject: Request for updating BIN(s) in AEPS Network

Dear Sir,

This is to inform you that the Bank has added new BIN(s) to its card base. Details have been furnished below:

BIN	Card Description (Platinum, Gold etc.)	Card Type (ATM, Debit, Prepaid, Credit)	Issuer Type (RuPay, VISA, Master Card etc.)	Card Length (16/19)	Card Technology (Mag / EMV)

We, hereby, declare that the above mentioned information is true to the best of our knowledge. The Bank assumes the onus of any interchange deviation arising due to wrong card type mentioned above.

We request to do the needful so as to route transactions with the above mentioned BIN(s) through AEPS.

Thanking you
Yours Sincerely

(Name & Designation -- Authorized Signatory)*

*Please note that the form should be affixed with the Bank seal.

RBI/2010-11/218

DPSS.CO.CHD.No. 695 / 03.01.03 / 2010-2011

September 29, 2010

The Chairman and Managing Director / Chief Executive Officer
Banks and Authorised Payment Systems

Madam / Dear Sir

Directive on Settlement and Default Handling Procedures in Multilateral and Deferred Net Settlement Systems under the Payment and Settlement Systems Act, 2007

A firm legal basis provides certainty and predictability which is important for the smooth functioning of payment systems. The systems and procedures in place need to have a legal basis, especially the method of determining settlement obligations of the participants and the point at which the settlement of obligations is deemed final and irrevocable. It is essential for all multilateral and deferred net settlement systems (both paper based and electronic) to have legal certainty for netting and settlement arrangements since there is a time gap between clearing (or processing) and settlement.

The Payment and Settlement Systems Act, 2007 (the PSS Act) and Regulations framed thereunder, has provided a firm legal basis for the process of netting and settlement finality. To amplify this, it has been decided to issue a directive on Settlement and Default Handling Procedures (enclosed) for compliance by all payment system providers and system participants covering all multilateral and deferred net settlement systems authorised by the Reserve Bank of India. This covers all the Bankers' Clearing Houses managed by various banks across the country.

Amendments to the Procedural Guidelines are being effected to reflect the changes necessitated by this directive.

These instructions are being issued under the powers conferred on the Reserve Bank of India by the PSS Act (Act 51 of 2007).

Yours faithfully

(G Padmanabhan)
Chief General Manager

Encl. : Directive on Settlement and Default Handling Procedures
in Multilateral and Deferred Net Settlement Systems

Enclosure to Circular DPSS.CO.CHD.No. 695 / 03.01.03 / 2010-2011
dated September 29, 2010

**Directive on Settlement and Default Handling Procedures
in Multilateral and Deferred Net Settlement Systems**

(Issued under section 10(2) of the Payment and Settlement Systems Act, 2007)

1. Introduction

- 1.1. Multilateral and deferred net settlement systems (like Cheques, ECS or NEFT) are critical payment system components handling substantial volumes and are popular among customers (because of convenience) and bankers (because of lower liquidity requirements). Netting also benefits the regulators, by virtue of reducing the size of credit and liquidity exposure of participant banks, thereby leading to containment of systemic risk.
- 1.2. It is essential for all such net settlement systems to have legal certainty for netting and settlement arrangements. It is also crucial for the transactions settled through such a system to have finality encompassing the relevant statutory prescriptions.
- 1.3. Finality, till recently, was achieved by way of adoption of Uniform Regulations and Rules for Bankers' Clearing Houses (URRBCH) and bilateral agreements entered into by the system providers with the system participants.
- 1.4. With the coming into force of the Payment & Settlement Systems Act, 2007 (the Act) and the framing of Regulations thereunder, the process of netting has got statutory recognition. Section 23 of the Act, provides for finality and irrevocability of settlement effected in accordance with such procedure as soon as the payment obligation, as a result of such settlement, is determined irrespective of whether or not such obligation is actually paid or not.
- 1.5. To amplify the aspect of finality of settlement and secure the multilateral and deferred net settlement systems with a default handling procedure, it is considered necessary to issue a directive on settlement and default handling procedures. Apart from clarifying the finality of settlement aspects, the directive will also bring in transparency in the default handling procedures and uniformity in default handling procedures across all the multilateral and deferred net settlement systems approved by the Reserve Bank of India (the Bank).
- 1.6. The directive also intends to provide adequate protection from settlement risk in multilateral and deferred net settlement systems, as also ensure compliance with international minimum standards for netting schemes.
- 1.7. This directive on settlement and default handling procedures in multilateral and deferred net settlement systems is being issued in exercise of the powers conferred on the Bank by section 10(2), read with section 23 of the Act.

2. Definitions

In this Directive, unless the context otherwise require,

- 2.1. "Clearing house" means a collective entity of member banks for speedy and economic collection and clearance of cheques or electronic instructions, which is governed by the URRBCH / Procedural Guidelines issued by the Bank.
- 2.2. "Recalculation" means a default handling mechanism in respect of payment obligations that are not settled after their record in the books of the settlement bank. In case of resort to recalculation all dues to and obligations of the defaulting bank will be reversed by the Clearing House (on a request from the settlement bank) as if the defaulting bank did not participate in clearing.
- 2.3. "Settlement bank" means the bank which maintains the settlement accounts of all the member banks for settlement of clearing and / or other obligations.
- 2.4. Other words and expressions wherever used in this directive shall have the meanings and intent assigned to them in the Act.

3. Procedure for determining settlement in multilateral and deferred net settlement systems

3.1. Determination of settlement

- 3.1.1. In case of cheque clearing, after closure of the prescribed clearing window, Clearing Houses shall arrive at the net settlement position for each bank. This is based on all the instruments that have been accepted by the Clearing House for arriving at the net settlement position.
- 3.1.2. At Clearing Houses where processing operations are carried out in the night or at a time when the settlement bank is not open for operations, the time for arriving at the net settlement position shall be one hour before the opening of the settlement bank for daily operations. The time available between the time of completion of processing and the time of arriving at the net settlement position, is to complete the administrative requirements, including ensuring that the net settlement position has been carried out correctly, the figures are accurately posted in the vouchers (to be sent to the settlement bank), the amounts are properly conveyed to the settlement bank and the like.
- 3.1.3. After opening of the settlement bank, a time window of thirty minutes shall be provided to the settlement bank for posting the settlement position. This time window of thirty minutes would enable banks to fund their accounts with the settlement bank so that the clearing obligations are smoothly settled.

- 3.1.4. For Clearing Houses where processing operations are carried out when the settlement bank is open for operations, the maximum time window from the time of arriving at the net settlement position by the Clearing House till the time of posting the settlement position in the books of the settlement bank for settlement of clearing obligations shall be thirty minutes.
- 3.1.5. In case of electronic multilateral and deferred net settlement systems (like Electronic Clearing Service, National Electronic Funds Transfer and the associated variants) where processing operations are carried out in night or at a time when settlement bank is not open for operations, the time for arriving at the net settlement position shall be one hour before the opening of the settlement bank for daily operations (as specified at 3.1.2 above). The clearing obligations will be taken up immediately for settlement as soon as the settlement bank is open for operations. The additional time window of thirty minutes provided at 3.1.3 above will not be available for electronic multilateral and deferred net settlement systems.
- 3.1.6. In case of electronic multilateral and deferred net settlement systems where processing operations are carried out when settlement bank is open for operations, the net settlement position after being arrived at, will be conveyed immediately to the settlement bank for settlement of clearing obligations. The time window of thirty minutes provided at 3.1.4 above will not be available for electronic multilateral and deferred net settlement systems.
- 3.1.7. Each Clearing House shall publicise the time at which the net settlement position will be arrived at by the Clearing House and the time at which the settlement will be posted in the books of the settlement bank for settlement. Member banks shall ensure availability of funds in their settlement account at the time of posting of the settlement position in the books of the settlement bank to meet their clearing obligations, and in any case within the time window, if any, stipulated by the settlement bank for settlement of the obligations.

3.2. *Posting of net settlement position in the books of the settlement bank*

- 3.2.1. The time between arriving at the net settlement position and the time of posting of the net settlement position in the books of the settlement bank shall, however, be as minimum as possible. This is to ensure early completion of settlement.

3.3. *Default handling procedure*

- 3.3.1. In case of inability of a member bank to fund its settlement account to meet the net settlement obligations, it is open for the settlement bank to extend clearing overdraft or accommodation (temporary or otherwise) at the request of the member banks so that the clearing obligations are settled in the books of the settlement bank. The process of extending the overdraft shall, however, be a bilateral arrangement between the defaulting member bank and the settlement bank. It shall also be open for a member bank to have bilateral arrangements for liquidity with other member banks as well. Such bilateral arrangements shall have to operate and be completed within the time window (specified at 3.1.3 and 3.1.4), stipulated by the settlement bank for settlement of the obligations.
- 3.3.2. In case of inability of a member bank to fund its settlement account to meet the clearing obligations, the shortfall in the settlement account shall be dealt with as a default situation and the default handling procedure shall be put into operation.
- 3.3.3. In case the settlement is guaranteed, the default handling procedure shall involve utilising the margin money, invoking the line of credit extended to the defaulting bank, activating the loss sharing mechanism or any other guaranteed mechanism. Nuances of operationalising the default handling procedure shall be as per the procedural guidelines of the individual multilateral and deferred net settlement systems.
- 3.3.4. In situations where the settlement is non-guaranteed in nature, the mechanism of recalculation of settlement shall be applied. As part of this procedure, the settlement bank will request the Clearing House (with appropriate consent from the President of the Clearing House) to recalculate the settlement.
- 3.3.5. As part of the process of recalculating the settlement, the Clearing House shall 'exclude' all the transactions (both receivables and payables) of the defaulting member bank as if the said bank did not participate in clearing.
- 3.3.6. The recalculated position shall be immediately conveyed to the settlement bank and posted in the books of the settlement bank.
- 3.3.7. In case any other member bank is unable to meet its clearing obligations consequent to recalculating of the settlement, the steps at 3.3.3, 3.3.4 and 3.3.5 above will be repeated.
- 3.3.8. The process of recalculation of settlement as above is considered part of the settlement procedure.
- 3.3.9. In case of default and consequent recalculation of settlement, if insolvency arises during the interregnum, the immediately preceding settlement reached shall be treated as final and binding.

4. Others

- 4.1. The series of steps outlined at Para 3 above shall have to be fully complied with until the entire process of settlement from the time of arriving at the net settlement position by the Clearing House till the time the settlement obligations of member banks in their accounts with the settlement bank are fully met has been completed.
- 4.2. If it is decided by the Clearing House to extend the clearing settlement for any reason, the Clearing House shall announce at the time of acceptance of instruments / instructions for settlement, the time up to which extension has been considered and the time at which the net settlement position is intended to be arrived at and communicated to the settlement bank.
- 4.3. Individual Clearing Houses may prescribe with the approval of the President of the Clearing House other measures such as net debit caps, presentation limits, etc., for mitigating risk of default by member banks. Such measures shall in no way impact the process of settlement as prescribed at Para 3 above.

5. Application of the directive

- 5.1. The directive shall be applicable to all multilateral and deferred net settlement systems like Cheques (at MICR-Cheque Processing Centres and other Clearing Houses, including Cheque Truncation System), Electronic Clearing Service (Debit, Credit and related equivalents, if any), National Electronic Funds Transfer system and the like.
- 5.2. With immediate effect, the directive shall be applicable and binding on all Clearing Houses, system providers, member banks of Clearing Houses, members of payment systems operated by the system providers and the banks maintaining settlement accounts of member banks. The directive shall be applicable to other payment and settlement products as determined by the Reserve Bank of India from time to time.
- 5.3. URRBCH and Procedural Guidelines as they exist for various multilateral and deferred net settlement systems shall, wherever a reference is contained, also mean and include the directive on settlement and default handling procedures contained herein.

Annexure-IV

ON STAMP PAPER

Letter of Authority

To,

The Regional Director,
Reserve Bank of India
Mumbai

Dear Sir,

Our Current A/c No. _____ and Settlement A/c No. _____ with
the Reserve Bank of India (RBI) Mumbai.

1. National Payments Corporation of India (hereafter referred to as the NPCI) has admitted us as member of a networking arrangement called the Aadhaar Enabled Payments System (AEPS) whereby switching and processing of all our electronic payments transactions over their network takes place under NPCI's guarantee of clearing and settlement of our transactions.
2. For that purpose, we hereby authorize and request that as and when a settlement instruction is received by you from the NPCI relating to our transactions in the said AEPS Network, you may, without reference to us, debit/credit our above Current Account/s with such sums as may be specified by the NPCI in its settlement instructions, notwithstanding any dispute that may exist or arise between us and NPCI.
3. The settlement instruction for debiting/crediting our Current Account/s with you shall be conclusive proof of debit/credit of our Current Account/s relating to our transaction in the said AEPS Network as referred to in paragraph 2 above and it shall not be necessary for us to admit and/ or confirm to the fact of such debit/credit by means of separate advice to you and/ or NPCI.
4. We hereby further unconditionally and irrevocably undertake to arrange for the requisite funds in our Current Account with Deposit Account Department, Reserve Bank of India, Mumbai to meet the demand of NPCI. We shall be bound by this undertaking and shall be liable therefore under all circumstances.
5. The mandate and undertaking shall not be revoked by us except with the prior concurrence of both the NPCI and the Reserve Bank of India (RBI) and you may act upon this mandate till such time this authority is revoked in writing and all actions taken by RBI in pursuance of this mandate shall be absolutely binding on us, without any risk or responsibility to the RBI.

Thanking you,

Yours faithfully,

For and on behalf of the Applicant

Annexure-V

NON-DISCLOSURE AGREEMENT

(On stamp paper)

This Agreement is made and entered on this ----- day of -----, 201 (“Effective Date”) between

NATIONAL PAYMENTS CORPORATION OF INDIA, a company incorporated in India under Section 25 of the Companies Act, 1956 and having its registered office at **1001A, B Wing, 10th Floor, The Capital, Plot 70, Block G, Bandra-Kurla Complex, Bandra (East), Mumbai - 400 051, Maharashtra**, (Hereinafter referred to as “NPCI”, which expression shall mean and include unless repugnant to the context, its successors and permitted assigns);

AND

_____, a company registered in _____ and having its registered office at _____ (Hereinafter referred to as “-----”, which expression shall mean and include unless repugnant to the context, its successors and permitted assigns).

The term “Disclosing Party” refers to the party disclosing the confidential information to the other party of this Agreement and the term “Receiving Party” means the party to this Agreement which is receiving the confidential information from the Disclosing Party.

NPCI and ----- shall hereinafter be jointly referred to as the “Parties” and individually as a “Party”.

NOW THEREFORE

In consideration of the mutual protection of information herein by the Parties hereto and such additional promises and understandings as are hereinafter set forth, the Parties agree as follows:

Article 1: Purpose

The purpose of this Agreement is to maintain in confidence the various Confidential Information, which is provided between NPCI and ----- to perform the considerations (hereinafter called “Purpose”) set forth in below:

(STATE THE PURPOSE)

Article 2: DEFINITION

For purposes of this Agreement, “**Confidential Information**” means the terms and conditions, and with respect to either Party, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to the Purpose (including, but not limited to, information identified as being proprietary and/or confidential or pertaining to, pricing, marketing plans or strategy, volumes, services rendered, customers and suppliers lists, financial or technical or service matters or data, employee/agent/ consultant/officer/director related personal or sensitive data and any information which might reasonably be presumed to be proprietary or confidential in nature) excluding any such information which (i) is known to the public (through no act or omission of the Receiving Party in violation

of this Agreement); (ii) is lawfully acquired by the Receiving Party from an independent source having no obligation to maintain the confidentiality of such information; (iii) was known to the Receiving Party prior to its disclosure under this Agreement; (iv) was or is independently developed by the Receiving Party without breach of this Agreement; or (v) is required to be disclosed by governmental or judicial order, in which case Receiving Party shall give the Disclosing Party prompt written notice, where possible, and use reasonable efforts to ensure that such disclosure is accorded confidential treatment and also to enable the Disclosing Party to seek a protective order or other appropriate remedy at Disclosing Party's sole costs. Confidential Information disclosed orally shall only be considered Confidential Information if: (i) identified as confidential, proprietary or the like at the time of disclosure, and (ii) confirmed in writing within Seven (7) days of disclosure.

Article 3: NO LICENSES

This Agreement does not obligate either Party to disclose any particular proprietary information; to purchase, sell, license, transfer, or otherwise dispose of any technology, services, or products; or to enter into any other form of business, contract or arrangement. Furthermore, nothing contained hereunder shall be construed as creating, conveying, transferring, granting or conferring by one Party on the other Party any rights, license or authority in or to the Confidential Information disclosed under this Agreement.

Article 4: DISCLOSURE

1. Receiving Party agrees and undertakes that it shall not, without first obtaining the written consent of the Disclosing Party, disclose or make available to any person, reproduce or transmit in any manner, or use (directly or indirectly) for its own benefit or the benefit of others, any Confidential Information save and except both Parties may disclose any Confidential Information to their Affiliates, directors, officers, employees or advisors of their own or of Affiliates on a "need to know" basis to enable them to evaluate such Confidential Information in connection with the negotiation of the possible business relationship; provided that such persons have been informed of, and agree to be bound by obligations which are at least as strict as the recipient's obligations hereunder. For the purpose of this Agreement, Affiliates shall mean, with respect to any Party, any other person directly or indirectly Controlling, Controlled by, or under direct or indirect common Control with, such Party. "Control", "Controlled" or "Controlling" shall mean, with respect to any person, any circumstance in which such person is controlled by another person by virtue of the latter person controlling the composition of the Board of Directors or owning the largest or controlling percentage of the voting securities of such person or by way of contractual relationship or otherwise.
2. The Receiving Party shall use the same degree of care and protection to protect the Confidential Information received by it from the Disclosing Party as it uses to protect its own Confidential Information of a like nature, and in no event such degree of care and protection shall be of less than a reasonable degree of care.
3. The Disclosing Party shall not be in any way responsible for any decisions or commitments made by Receiving Party in relying on the Disclosing Party's Confidential Information.

Article 5: RETURN OR DESTRUCTION OF CONFIDENTIAL INFORMATION

The Parties agree that upon termination of this Agreement or at any time during its currency, at the request of the Disclosing Party, the Receiving Party shall promptly deliver to the Disclosing Party the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Receiving Party or its Affiliates

or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

Article 6: INDEPENDENT DEVELOPMENT AND RESIDUALS

Both Parties acknowledge that the Confidential Information coming to the knowledge of the other may relate to and/or have implications regarding the future strategies, plans, business activities, methods, processes and or information of the Parties, which afford them certain competitive and strategic advantage. Accordingly, nothing in this Agreement will prohibit the Receiving Party from developing or having developed for it products, concepts, systems or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in the Confidential Information provided that the Receiving Party does not violate any of its obligations under this Agreement in connection with such development.

Article 7: INJUNCTIVE RELIEF

The Parties hereto acknowledge and agree that in the event of a breach or threatened breach by the other of the provisions of this Agreement, the Party not in breach will have no adequate remedy in money or damages and accordingly the Party not in breach shall be entitled to injunctive relief against such breach or threatened breach by the Party in breach.

Article 8: NON-WAIVER

No failure or delay by either Party in exercising or enforcing any right, remedy or power hereunder shall operate as a waiver thereof, nor shall any single or partial exercise or enforcement of any right, remedy or power preclude any further exercise or enforcement thereof or the exercise of enforcement of any other right, remedy or power.

Article 9: DISPUTE RESOLUTION

If any dispute arises between the Parties hereto during the subsistence or thereafter, in connection with or arising out of this Agreement, the dispute shall be referred to arbitration under the Indian Arbitration and Conciliation Act, 1996 by a sole arbitrator mutually agreed upon. In the absence of consensus about the single arbitrator, the dispute may be referred to joint arbitrators, one to be nominated by each Party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. Arbitration shall be held in Mumbai, India. The proceedings of arbitration shall be in the English language. The arbitrator's award shall be final and binding on the Parties.

Article 10: GOVERNING LAW AND JURISDICTION

This Agreement shall be governed exclusively by the laws of India and jurisdiction shall be vested exclusively in the courts at Mumbai in India.

Article 11: NON-ASSIGNMENT

This Agreement shall not be amended, modified, assigned or transferred by either Party without the prior written consent of the other Party.

Article 12: TERM

This Agreement shall remain valid from the effective date until the termination of this Agreement. The obligations of each Party hereunder will continue and be binding irrespective of whether the termination of this Agreement for a period of three (3) years after the termination of this Agreement.

Article 13: INTELLECTUAL PROPERTY RIGHTS

Neither Party will use or permit the use of the other Party's names, logos, trademarks or other identifying data, or infringe Patent, Copyrights or otherwise discuss or make reference to such other Party in any notices to third Parties, any promotional or marketing material or in any press release or other public announcement or advertisement, however characterized, without such other Party's prior written consent.

Article 14: GENERAL

1. Nothing in this Agreement is intended to confer any rights/remedies under or by reason of this Agreement on any third Party.
2. This Agreement and the confidentiality obligations of the Parties under this Agreement supersedes all prior discussions and writings with respect to the Confidential Information and constitutes the entire Agreement between the Parties with respect to the subject matter hereof. If any term or provision of this Agreement is determined to be illegal, unenforceable, or invalid in whole or in part for any reason, such illegal, unenforceable, or invalid provisions or part(s) thereof shall be stricken from this Agreement.
3. Any breach of any provision of this Agreement by a Party hereto shall not affect the other Party's non-disclosure and non-use obligations under this Agreement.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement by their duly authorized representatives as of the Effective Date written above.

NATIONAL PAYMENTS CORPORATION OF INDIA TYPE COMPANY NAME

By:

By:

Name:

Name:

Designation:

Designation:

Annexure-VI

On Letter Head.

KYC/AML Undertaking

We _____ (Name of the Member) with registered office at _____ have agreed to participate in the implementation of the products & services provided by National Payments Corporation of India (NPCI), with registered office at 1001 A, B wing 10th Floor, The Capital, Bandra-Kurla Complex, Bandra (East), Mumbai - 400051 and for that purpose, We hereby declare and undertake to NPCI that:

We hereby confirm to have an established process for Know Your Customer (KYC), Anti Money Laundering process (AML) & Combating of Financing of Terrorism (CFT) and that we shall comply with all the Reserve Bank of India (RBI) norms on KYC, AML & CFT.

We hereby confirm that none of our | the company's Director(s) is/are a "Politically Exposed Person (PEP)" or "close relative(s) of a PEP" or appear in the "list of terrorist individuals / entities" provided by RBI. In the event of our existing Director(s) is/are "PEP" or "close relative(s) of a PEP" or appear in the list of "terrorist individuals / entities" provided by RBI, the details of same shall be furnished to NPCI on letter head .

We hereby confirm to have an appropriate procedure for PEP check and name screening of employees and customers against the list of terrorist individuals / entities provided by RBI. In the event of an existing employee(s), customer(s) or the beneficial owner(s) of an existing account, using NPCI products & services, is a "PEP" or "close relative(s) of a PEP" or appear in the list of "terrorist individuals / entities" provided by RBI, we confirm to provide the details of such employee(s)/customer(s) or beneficial owner(s) to NPCI.

Keeping in view the new regulatory guidelines of Reserve Bank of India, we hereby confirm to have appropriate ongoing risk management procedures for Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) in case if any customer(s) or the beneficial owner(s) of an existing account is/are a "PEP" or "close relative(s) of a PEP" or appear in the list of "terrorist individuals / entities" provided by RBI.

We hereby confirm to offer NPCI products & services only to the customers who are KYC compliant.

We hereby confirm to do the necessary investigation and provide NPCI with the required details on alerts sent to the bank by NPCI's Risk Management Team.

Date:

Authorized Signatory (ies)

Place:

(Name & Designation)

(With Stamp)

**** End of Document ***