NPCI /UPI/OC No. 32/2017-18 **15th September 2017**

To,

All Member Banks - Unified Payments Interface (UPI)

Dear Sir/Madam,

Subject: Unified Payment Interface: Multiple bank model (API Approach)

This circular enables multi-bank PSP model, in which a large merchant/tech player (referred as "third party app provider") having an access to large customer base, can connect to UPI system through multiple PSP banks. In the multi-bank API arrangement, NPCI shall provide the NPCI Common Library (CL) directly for integration to the third party app provider on behalf of PSP banks. The App connects to PSP bank systems through third party app provider's system using API on secure channel.

For initiation, the third party app provider needs to write to NPCI with the names of participating banks (up to maximum of 5 banks). The letter should also include the details of existing user base and volume commitment.

The participating banks must note the following:

A. **Storing customer data by app provider systems in Multi-bank model**: We classify the data into two types, namely 'Customer data' and 'Customer payment sensitive data':

1. **Customer Data (including customer consented data)**:
   The customer data can be defined as Customer's name, customer's mobile number, residential address, email ID, gender, location details (entered by customer); device details such as App id, IMEI number, transaction related details – UPI ID, RRN, transaction id, time stamp, beneficiary UPI ID, beneficiary account number and beneficiary CBS name resolved by beneficiary's PSP (stored for subsequent transaction enablement) etc. **The UPI transaction data should be stored in the app providers system in encrypted format.**

2. **Customer payment sensitive data**:
   Classified as customer account details (such as Account number) customer payment authentication data (such as device fingerprinting) required for authentication as first factor. **This data can be only stored in PSP bank systems.** Some of the data like account number, can be shown in masked format to the customer on the app as per existing UPI PG. **Last 6 digits of the Debit Card, Expiry date of the debit card, UPI PIN, Issuer OTP should not be stored.**

B. **PSP Bank's ownership & responsibility:**

1. The App provider shall provide the required documentation including data flow diagram, security details to PSP bank and NPCI.
2. The PSP bank must ensure that its board approves such multi-bank arrangement, since all the liability arising in case of any data breach, wrong authentication etc. is borne by

PSP banks. The board resolution shall be submitted to NPCI as part of onboarding process.

3. All data exchange between the app, the app providers system and PSP bank shall be through a secure channel.
4. The PSP bank shall continue the authentication, encrypted SMS OTP verification as detailed out in the current PSP SDK guidelines.
5. It is assumed that the data for device binding shall come from the app and the third party app provider. The bank must ensure that the system and app audit performed to ensure data integrity, encryption and the app security. This audit shall be done on annual basis.
6. PSP Banks shall have the full right to conduct audit on the third party App provider infrastructure, systems, application and database for components related to UPI.
7. PSP Bank shall ensure that it will facilitate RBI, NPCI or any other formally appointed agencies of RBI/ NPCI, to access the data and carry out audits of Bank and third party app provider, as and when required.
8. The PSP bank must have agreement with third party App provider for any liability arising out of data breach/fraud/compromise at the app or third party app provider's system. Further the agreement/ arrangement between bank and third party app provider must include compliance to Informational Privacy (as aspect of Right to Privacy), IT act, Payment and Settlement System Act, UPI Procedural guidelines or any such future law and guidelines issued by government of India, RBI, any other regulator in India and NPCI.
9. The PSP bank must provision for customer to raise disputes on the app and should ensure complaint management processes as per UPI Operating and settlement guideline and Operating Circulars. The third party app provider and PSP bank must ensure the customer service in case of disputes as prescribed by UPI procedural guidelines and RBI customer service guidelines issued time to time.
10. The call center number (toll free number in India) must be prominently displayed on the app for customer service.
11. PSP Bank should ensure that all UPI Customers could participate to use this app & choose any bank account from the list of Banks available on UPI platform.
12. PSP Bank shall ensure that that third party app provider shall require an exclusive permission from NPCI & PSP bank for sharing individual UPI transaction data with any other third party including its own Parent, subsidiaries and subsidiaries of parents other than entities such as - Indian Government/Indian intelligence/Indian law enforcement agencies/Indian regulatory bodies.
13. PSP Bank shall ensure that Customer can get the handle of the bank where he/she has their account, by default; and for or all other bank customers (i.e. other than the participating banks) this allocation happens at the back-end on a fair distribution method as agreed between PSP Bank and the third party app provider. Any changes in the handle allocation rule shall require explicit approval of NPCI. In case the handle of the default bank cannot be made available for technical reasons, the handle may be allocated through the fair allocation method.
14. PSP Bank shall ensure that the customer has the choice of changing the handle later through appropriate enablement in the app.

15. PSP Bank shall ensure that the third party app provider shall take explicit customer consent for using transaction data for themselves and/or PSP bank for the purposes such as - Cross-Sell/ Promotions/ Offers/ Value Added Services/Increasing Transactions/Better User Experience/such other purposes as shall be approved by NPCI in writing.
16. PSP Bank shall ensure that the third party app provider will ensure that no application version with significant UPI related changes shall go live without a formal assessment and approval, excluding minor changes and bug fixes. Any major change can be qualified as major functionality change in UPI offering OR security related change that shall require audit and be governed basis the arrangement between PSP Bank & third party app provider.
17. PSP Bank and/or third party app provide shall not route any interbank transactions within themselves.
18. PSP Bank shall ensure that the details of beneficiary customer such as account number and CBS name shall not be used by third party app provider other than for transaction processing.
19. For instances wherein the third party app provider's data resides outside the country, either the SOC 2 compliance audit report or a reputed third party auditor's report as per scope defined by NPCI and banks needs to be submitted to NPCI and PSP banks.
20. PSP Bank will give reasonable assurance or undertaking directly by the PSP Bank or from third party app provider that the app is adequately secured.

Rest of the conditions listed in the existing UPI guidelines shall continue to apply as is.

Thanking you,

Yours faithfully,

Dilip Asbe
Chief Operating Officer