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

To,
All Member Banks - Unified Payments Interface (UPI)

Dear Sir/Madam,

Subject: Single PSP model Merchant integration (Addendum circular 15B)

In addition to Bank PSP apps, adoption of UPI payment by merchants and third party app providers has enabled the growth of UPI by integrating PSP SDK into their app. This entails bank to share the Common Library (CL) in a secured wrapper within PSP SDK (Software development kit). The PSP bank SDK integrated in the app connects to the bank PSP server for UPI related functions on secure channel. This circular to be read in continuation to 15 and 15A.

The banks engaging in deep integration with third party app provider should note the following;

a) **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.**

b) **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.**

PSP Bank ownership & responsibility (Additional):

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 PSP SDK arrangement, since all the liability arising in case of any data breach, wrong authentication etc. is borne by the PSP bank. The board resolution shall be submitted to NPCI as part of onboarding process.
3. The PSP bank shall continue the authentication, encrypted SMS OTP verification as detailed out in the current PSP SDK guidelines.

4. The bank must ensure that the system and app audit is performed to ensure data integrity, encryption and the app security. This audit shall be done on annual basis.

5. PSP Bank shall have the full right to conduct audit on the third party App provider infrastructure, systems and application, database and security practices including access/ user/ incident/ management at their end for components related to UPI.

6. 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.

7. The PSP bank must provide all the documentation and audit reports as listed by NPCI before go live of any such third party app on single SDK model.

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 centre 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 third party app provider shall require an exclusive permission from NPCI & PSP bank for sharing individual UPI transaction data and UPI related customer details 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 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.

14. 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.

15. 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.

16. 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 needs to be submitted to NPCI and PSP bank.

17. 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.

For the existing arrangements on the PSP SDK model, PSP Banks need to ensure complete compliance to the above stated, latest by 31st of December 2017.

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