NPCI

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

NPCI /UPI/OC No.15/2016-17

January 18, 2017

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

Dear Sir/Madam,

Subject: UPI Merchant SDK: Specific requirements & Compliance

Your attention is drawn on following,

2) NPCI has communicated the PSP SDK guidelines wide email dated on 30th Nov and circular no. NPCI/UPI/OC No. 12/2016-17 dated December 1st 2016 under the subject "Compliance to Merchant Onboarding and SDK guidelines checklist". The compliance directives and the corresponding dates are summarized again for your prompt action:

Sr.	Compliance	Outer date
1	Security Audit of SDK Code base of banks	BY 31/12/2016
2	Compliance of functionality & flow used in PSP SDK guidelines specially on interoperability for customers & merchants for merchant apps	By 31/01/2017
3	Security compliance of all merchant apps where SDK	By 28/02/2017

3) With regard to SDK security assessments / certification as a part of on-boarding, your reference is drawn to our Compliance circular no. NPCI/2017-18/RMD/001. The circular provides the scope and empaneled vendors for security assessments http://www.cert-in.org.in/PDF/Empanel.org.pdf. Merchant acquiring bank shall conduct external security audit of PSP SDK and submit the report to NPCI. Merchant acquiring bank, shall also give undertaking for each of the merchant app security (where its PSP SDK integrated) to NPCI, before it is launched.

4) Complete ownership of compliance and security of merchant app continues to remain with the merchant acquiring / PSP SDK owner bank.

5) In the web merchant, after the selection of "pay by UPI" option, the equal preference is given to the customer to enter his VPA for collect call.

6) Reiterating some of the broad guiding principles with regard to the PSP SDK: (Kindly refer to the complete guidelines for full details)

   a) Only Bank led Apps be called "UPI PSP Apps" and merchant / 3rd party p2p provider Apps shall be called "UPI compliant Apps"

b) Banks are allowed to supply PSP SDK to their acquired merchant provided banks have the board approval to play this role, since it involves taking full liability in case of issues/breach in the merchant app.

c) Some of the interoperability principals for PSP SDK integrated merchants: (Kindly refer guidelines for full details)

   a. UPI Registration: No merchant can / shall force the customer to create a VPA / register for UPI to avail any services on merchant app.
   b. Payment: The merchant should allow the customer to enter his/her VPA as an equal choice / option and not force creation of VPA for purchase / utilizing the services on merchant app.
   c. The PSP SDK where customer has registered on UPI, should respond to an intent call from any other UPI enabled App on the same phone
   d. The PSP SDK onboarding and payment pages should only have branding of the PSP bank.
   e. The PSP SDK should also give option to customer to de-register / delete his/her VPA.
   f. The PSP SDK, can give an option to customer to the registered his handle as default provided the customer has chosen explicitly (the default option should be pre-checked on NO) for the purpose of payment on this specific merchant. If the customer has chosen 'Yes" then the PSP SDK is absolved from calling an intent call, only for that merchant transaction. The customer should have the choice to change his selection of default option either way during the life cycle.
   g. The customer data shall continue to reside in bank or bank owned data center. The authentication is only done by PSP bank in all UPI scenarios.
   h. The PSP bank should not share any customer data with the merchant unless specified by industry regulator for e.g. SEBI, IRDA for brokers, mutual funds, and insurance.
   i. Banks shall not share NPCI library in open format and it should be integrated in the PSP SDK before sharing.

It may please be noted and as highlighted earlier, if the merchants or third party p2p providers remain non-compliant on guidelines stated by the timeline, NPCI will have an right to decline the transactions without any prior notice.

Thanking you,

Yours faithfully,

Dilip Asbe
Chief Operating Officer