NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

NPCI/UPI/OC-15A/2016-17 **January 27th, 2017**

To,
All Member Banks - Unified Payments Interface

Dear Sir/Madam,

Checklist for PSP SDK- Addendum to circular 15

As discussed in IBA meeting & UPI Steering Committee, NPCI had issued broad guidelines for merchant on-boarding to member Banks on 30th November 2016. It was followed up with UPI Circular No. NPCI/UPI/OC-13/2016-17 dated 8/12/16 &NPCI/UPI/OC-15/2016-17 dated 18/1/2017 respectively, reiterating compliance to 'Merchant on-boarding guideline & SDK Checklist'.

Matter has been reviewed in consultation with Reserve Bank of India. Accordingly the following checklist should be submitted to NPCI on a signed letter-head, both for existing and new merchants/P2P providers.

Sr. No.	UPI Interoperability principals for SDK integration & web enablement	Compliance status (Y/N)
1)	Bank Board approval in place for distribution of SDKs to large merchants or P2P provider. (As bank needs to assume all liabilities due to breach / security issues in merchant or P2P provider app).	
2)	Name of the merchant/P2P provider:	
3)	"Pay by UPI" is equally placed along with other payment options (such as cards / net banking etc) on merchant / P2p provider on App/Web.	
4)	PSP SDK app should not mandate the customer to register for UPI or create VPA to avail product or services provided. (Enabling condition for other VPA's to be accepted)	
5)	Merchant/P2P provider must give equal choice to the customer to pay by VPA of his choice i.e. registered VPA in SDK or any other VPA customer has. (Merchant/P2P provider to use intent or collect call on App and collect call on web to facilitate customer to use VPA of his choice)	
6)	PSP SDK must respond (once customer has registered successfully) to intent calls and collect calls.	
7)	PSP SDK must provide an option to customer to de-register & delete VPA (life cycle management)	
8)	PSP SDK to provide an option to customer to register the handle as 'default' for payment on this specific app during on-boarding process.	
a)	The 'Default' option provided should be pre-checked on 'No'	
b)	If customer has chosen 'Yes', then the PSP SDK is absolved from mandated intent / collect call only for that "merchant or P2P provider services".	

1001A, The Capital, B Wing, 10th Floor, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. T: +91 22 40009100 F: +91 22 40009101 www.npci.org.in
CIN : U74990MH2008NPL189067

Sr. No.	UPI Interoperability principals for SDK integration & web enablement	Compliance status (Y/N)
c)	Provision to allow customer to alter the 'Default' option during the life cycle (Change the option chosen earlier)	
9)	PSP SDK on-boarding and payment pages should only have branding of the PSP bank.	
10)	PSP bank is not sharing any customer data with the merchant/P2P provider, unless specified by industry regulator. E.g. SEBI, IRDA etc. (permitted only for specific regulated merchants). No authentication data shared outside PSP bank.	
11)	Sharing of NPCI common library is within a wrapper in the SDK for integration purpose (and not given 'open')	
12)	PSP banks should ensure that Merchant / P2P provider Apps are called as "UPI Compliant Apps" and not "UPI PSP Apps"	
13)	All above features, must be verified by "Bank's Compliance Team" and given their sign off in writing to bank's UPI business/technology team to on-board this merchant/P2P provider with PSP SDK.	

Sr. No.	Security compliances and other essentials	Compliance status (Y/N)
1)	Banks to conduct third party (list guided by NPCI circular) security audit of PSP SDK code base and submit the clean audit report to NPCI (one time activity unless major changes done thereafter). If major changes done, it is mandatory for bank do redo the activity. a) First time report b) Next release	
2)	"Bank's Audit Team" must have given signoff in writing to bank UPI business/technology team to go live for this merchant/P2P provider. (The PSP SDK integrated merchant or P2P provider final app, must go through the third party security audit and Bank audit team must have verified the compliance and obtained clean report)	
3)	The data pertaining to customer (including the account details) & device finger printing, resides in bank Data Centre or bank controlled Data centres / Servers with access by bank authorised personnel only.	

As indicated in the circular NPCI/UPI/OC - 15/2016-17 dated 18th January 2017 that merchants /P2P provider not following guidelines on interoperability or security, transactions shall be declined by NPCI centrally.

Kindly ensure compliance.

Yours faithfully,

Dilip Asbe
Chief Operating Officer