NPCI
भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

NPCI/UPI/OC No. 05 / 2016-17 **6th September 2016**

All Member Banks, Unified Payments Interface (UPI)

Dear Sir / Madam,

Subject: Security Considerations on 'Unified Payments Interface (UPI)' – Immediate Actions

1. UPI provides for flexibility to the end customer in terms of creating a Virtual Address. Accordingly a VPA like 1234567@abcbank is a valid VPA for a PSP. It is also possible that the customer may create virtual address with his Mobile Number / Aadhar number as well which are numeric and easy references for him/her. *(Ref: Sub point 3; section 2.1 'Core features' of the UPI Tech Specifications Ver 1.2.3).*

    a. UPI provides for an API ***'ReqValAdd'*** basis which the name of the customer as registered with the PSP can be checked and member banks are providing this facility already.

    b. However, in case of use of 'Mobile Numbers' as the Virtual address by the end customer, we wish to advise that the PSPs may permit only the same Mobile number to be opted as VPA by the customer for e.g. (9123456789@abcbank) for which the sms has been sent at the time of registration. The PSP should validate this mobile number before permitting the creation of Virtual address. This is an important step towards containing any fraud risk should a gullible customer not notice the Mobile number change OR mis-representation by any fraudster.

2. UPI PSP Apps provide for an option to the customer for resetting his App login password/PIN.

    a. While some banks follow an authentication mechanism using private questions OR sending rest password over registered email, there are Apps which provide for resetting of passwrod where the initiation & delivery of the Reset Password is on the Mobile Chanel itself.

    b. With reference to the above and in order to provide for higher security on UPI, it is expected that the member banks provide for an out of band ("Not mobile") based authentication of the customer before etting him reset the password. This is aimed at containing the risk for the UPI customers.

3. Please refer NPCI Circular no.s NPCI/UPI/OC No. 03/2016-17 dated 2nd of August 2016 under the subject "Daily reconciliation of UPI transactions' & sub point (b.4) vide our NPCI/UPI/OC No. 04/2016-17 dated 12/08/2016 under the subject "Compliance with the NPCI Circulars and Procedural Guidelines of UPI".

NPCI has amply highlighted the importance and criticality of daily automated reconciliation of UPI transactions through these communications. However, we understand that many banks are yet to deploy automated reconciliation for UPI. This is a critical actitiy and we reuest member banks on UPI to accord this top most priority.

We shall be grateful to have a confirmation from our member banks on the above. Your responses and confirmations in this regard may please be forwarded to the email id : Ms Sarika Sorte sarika.sorte@npci.org.in

Yours faithfully,

Dilip Asbe
Chief Operating Officer