Circular: NPCI/2020-21/BBPS/003 **April 28th, 2020**

To,
All BBPOUs
Bharat Bill Payment System

Mandatory Technical Standards & Regulatory Observations

Dear Sir / Madam,

This is with reference to the Mandatory Technical Requirements of BBPS and Regulatory observations, the key findings are delineated as under:

Information Security:

Over a period of time, the minimum standard for 'Cryptographic Protocol' has moved away from TLS* 1.1 to TLS 1.2, similarly 'Cryptographic Hash' function has moved away from SHA#-1 to SHA-2, based on regulatory audit direction you are advised to adhere to the below mentioned latest Cryptographic Standards on top most priority:

1. **Cryptographic Protocol:** All the BBPOUs should enforce at least (TLS 1.2) 256-bit encryption level for all BBPS Transactions.
2. **Cryptographic Hash Function:** All the BBPOUs must use a hash function SHA-2 (at least SHA-256 or above) only, in order to ensure data integrity.

Risk Management:

Currently BBPS Technical standards permit to on-board the COU & BOU services through a single natted IP address. Here there is a risk of compromise in one function impacting the other. Hence as per the revised standards, BBPOUs are advised to segregate the COU & BOU services separately through two different & independent IP addresses, so that one function should not impact the other. Those BBPOU entities servicing a large number of COU / BOU entities are requested to get in touch with us and we will be glad to work together on a proper segregation plan (COU / BOU bifurcation) based on your business sensitivities & priorities.

The above mentioned observations are associated with Information Security, Risk Management and also flagged by the Regulators, the BBPOUs are advised to implement the recommendations on a priority basis confirming compliance by 25th May 2020. We will be glad to engage with you in accomplishing this at the earliest.

Recommendation:

It is highly recommended that BBPOUs take requisite precautions to ensure that IT Infrastructure induced performance limitation should never hamper the smooth BBPS transaction processing. A separation between the BOU & COU IT infrastructure is recommended.

* TLS – Transport Layer Security
# SHA – Secure Hash Algorithm

Yours faithfully,

Arulananda Selvakumar
Head - Technology, BBPS
National Payments Corporation of India