NPCI/2024-25/BBPS/005 **15th August 2024**

To
All BBPOUs
Bharat Bill Payment System,
NPCI Bharat BillPay Ltd.

Dear Sir / Madam,

Subject - Data Security and Privacy Standard Framework for Credit Card Bill Payment Transactions processed through BBPS

The Bharat Bill Payment System ("BBPS") remains dedicated to offering an integrated, accessible, and interoperable bill payment system that is safe, secure, and resilient. It has been our endeavour to safeguard critical, personal and sensitive data of customers. The authorised Operating Units (OU's) shall be responsible for their systems, data usage and privacy related guidelines including that of their Agent Institutions (AI's), Participating AIs, Agents and Service Providers connected to the BBPS platform through them. This circular addresses the data security and standards for Credit Card Bill Payments.

1. **Data Classification and Storage:**
   - **a.** Customer Data should be classified as:
     - i. Customer-Consented Data (e.g., Customer Name, combination of last 4 digit of card number, credit card bill details), to be stored in encrypted form with customer consent in a time bound manner.
     - ii. Customer Sensitive Data (e.g., PINs, passwords/One-time passwords, card number in full, Customer account or balances,) cannot be stored even in encrypted format.
     - iii. Non-Personal / Non-PII data (e.g., transaction number, transaction amount) can be stored and transmitted in secure format as per the OU's internal policy and in adherence to the secure data standards using latest encryption algorithms.

2. **Data usage guidelines:**

   - **a.** All OUs including their AIs, Participating AIs, Agents and Service Providers, must process only "customer initiated" fetch transactions for credit card bill payments. It is advised that the first such fetch transaction is duly authenticated, to ensure the customer has accessed the accurate mobile number and card number combination.
   - **b.** The fetch and reminders should be processed only basis an explicit and time bound customer consent, with suitable opt out option for the customer.

c. The bill details such as actual / updated balance, outstanding balance, due date and minimum amount due or any such details that are returned by BBPS systems from the Credit Card issuer, based on consumer request, must be used only to display to the customer on the mobile app or the website. It cannot be used directly or indirectly for any purpose other than displaying to the customer. Furthermore, this data needs to be purged in a time-bound manner beyond the consented duration.

3. Compliance to existing rules and applicable laws:

a. BBPOUs including AIs, Participating AIs, Agents, and Service Providers must comply with the RBI directive as per circular DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 6, 2018, and FAQs dated June 26, 2019 and the applicable payment data must be stored within India as per RBI data localisation guidelines.

b. Customer Data must reside in OU / AI / Participating AI owned or controlled systems, accessible only by authorized personnel employed with OU / AI / Participating AI.

c. Data security, privacy and access management controls (e.g., data encryption, masking, data leakage prevention, data access monitoring) must be implemented in accordance with all extant RBI, BBPS and the GOI applicable laws (including Digital Personal Data Protection Act, 2023), regulations and circulars issued time to time.

d. In order to make credit card bill payment transactions more secure and safe for the ecosystem, the COUs (and their AIs, Participating AIs, Agents and Service Provider) are required to capture the available remitter details for sharing with the issuers. **The requirement of passing remitter details by COUs is in accordance with Section 64 of Master Direction - Know Your Customer (KYC) Direction, 2016.**

e. UPMS must be implemented by all OUs (and their AIs, Participating AIs, Agents and Service Provider) to ensure incorrect reminders are not sent to customer once payment has been made.

Members are requested to take a note of this circular and ensure implementation in accordance with Annexure A given for compliance.

Yours Sincerely,
Sd/-
Noopur Chaturvedi
Chief Executive Officer (CEO)
NPCI Bharat BillPay Ltd.

Annexure – A

Sr. No.	Particulars	Timeline
1	Customer initiated fetch compliance	15th September 2024
2	Implementation of facilitating remitter information	30th September 2024
3	Mandatory and optional fields	30th September 2024
4	UPMS implementation	30th September 2024

NPCI Bharat BillPay Limited
(A wholly owned subsidiary of NPCI)
Registered Office: 1001 A, The Capital, B Wing 10th Floor, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. T: +912240009100 F: +91 22 40009101
Email id: bbps@npci.org.in
Website: www.bharatbillpay.com,
CIN: U6719OMH2O2OPLC351595