Inputs on MeitY 'Security of Prepaid Payment Instrument Rules 2017- Draft'

I. Overall Comments

1. DSCI-NASSCOM are thankful to the Ministry of Electronics and Information Technology (MeitY) for taking a lead in drafting guidelines for enhancing Security of Prepaid Payment Instruments (PPI) and deeply appreciate process of inviting comments from stakeholders for further refinement.

2. It is heartening to learn the rapid developments in past one year pushing the 'cyber security envelope' in the country, especially in the financial sector, which clearly signifies the focus of the governments and regulators in dealing with the menace of cyber security head on and enhancing trust and assurance in using the system - the Union budget advocates setting up of a **CERT-Fin for financial services**; CERT-IN launched '**Cyber Swacctha Kendra**'; Regulators in financial services like **RBI have published Cyber Security Framework** and very recently constituted a '**Cyber Security Panel**' of experts to review cyber security and digital threats environment in digital payment ecosystem; **IRDAI has published detailed cyber security framework** for their member organizations etc.

3. **DSCI-NASSCOM and member organization agree that security and privacy protection are very pertinent & critical to the proliferation of Digital India**, and in transformation to a less-cash society. Organizations are committed to ensuring security & privacy of customer data & transactions, and to mitigating security risks. We believe that **there is an urgent need to enhance Privacy Regime of the country by enacting a comprehensive Data Privacy Law in the country** to protect the entire ecosystem, not just one aspect.

4. We reached out to our member organizations operating in this space for their inputs. From an industry viewpoint, there appears an overlap of security conditions issued by the regulators like RBI for PPI ecosystem as RBI has also stipulated "**Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers**". In the consultation meeting hosted by MeitY, RBI mentioned that it is in the process of formulating a holistic framework for the PPI ecosystem. Industry is also of the view that there should be **only one government/regulatory body** which regulates the digital payments sector. Other govt. bodies will definitely have a role to play, but that should be confined within the existing regulatory framework. It is critical for the PPIs to comply with **simple, standardized and streamlined one set of security related regulatory requirements** instead of following multiple, often conflicting requirements issued by different govt. and regulatory bodies. It is important to note that the Watal Committee recommended regulation of digital payments to be independent from the function of central banking and suggested constitution of a more independent **Payments Regulatory Board (PRB)** within RBI. The PRB would govern all aspects of digital payments, including security and privacy.

5. By virtue of ePPI being "Body Corporate" (as defined in the IT Act), Sec 43A **Reasonable Security Practices and Procedures Rules are applicable** on them.

6. Security rules for any ecosystem should be formulated and stipulated in such a way that it should not inhibit market development & its dynamics. The guidelines should be **technology-agnostic, based on principles** and should take into account continual technological innovation without prescribing specific security or technical solutions. Such an open, non-prescriptive approach is the most adequate in allowing e-PPI issuers to design and implement effective solutions to ensure continued security in an environment of evolving technology and risk. A high level security framework should be leveraged for security implementation as the implementations may vary due to factors such as size of the organization, business model and technology developments etc. In addition, adoption of globally accepted standards allow businesses to scale and stay competitive without compromising compatibility across the world (eg. Paytm recently launched its services in Canada).

7. We believe that there is a need to develop overall guiding principles of **high level security framework for overall digital payment ecosystem in India** (last year G7 countries published a cybersecurity frameworks for the financial sector), than focusing on just one aspect of digital payment ecosystem. In an interconnected ecosystem, some of them have the potential of becoming a gateway to other financial facilities. Hence, **stipulating different regulatory security rules for distinctive use cases** such as ePPI may prove to be counterproductive from a market standpoint. By defining new regulatory requirements specifically for e-PPIs under the IT Act, the **regulatory level playing field** between e-PPIs and other payment players in the industry might get distorted.

8. It appears that some of the sections - 7,8,9 etc. – talk about '**personal information**' and seemingly go beyond the scope of the rule-making powers under the IT Act, given that section 43A and earlier issued "**Reasonable Security Practices and Procedures**" Rules are applicable for **Sensitive Personal Data or Information (SPDI)** and does not extend to "**Personal Information**" (as explained in the clarification issued by MeitY on Sec 43A Rules). Section 72A which provides punishment for disclosure of personal information in breach of a lawful contract is applicable to all organizations sharing "Personal Information" with an intent to cause wrongful loss or gain. Hence clarity on whether 43A Rules cover "PI" as scope, instead of "SPDI" needs clarification.

9. Keeping all the above pointers in mind and taking note of simultaneous developments happening in this space, **we request MeitY to issue the finalized draft as an "Advisory"**, similar to earlier issued 'Advisory on functioning of Matrimonial Websites'. **RBI should take this Advisory into consideration while devising the overall framework to avoid any inconsistency.**

II. Section Specific Comments (for inclusion in advisory)

2. Definitions

- Rule 2 (c) - Authentication data: The flexibility with respect to the manner in which authentication should be done or the factors used for authentication should be left up to the Issuer. Reference should be taken from RBI guidelines that allow the Issuing Banks the flexibility to determine the manner of authentication for card not present transactions. The definition proposed to be modified as follows: "*any information relating to the customer that may be used for the purpose of "authentication", which may include passwords, OTPs, Aadhaar numbers, biometric attributes or any other data that may be used for authentication as determined by the e-PPI Issuer*".

- Rule 2 (e), (f) and (g), these 3 definitions overlap with each other and cause interpretational concerns. Further, Definition of Cyber Incident and Cyber Security Incident are different in Sec 43A Reasonable Security Practices and Procedures Rules and these Rules. **It is proposed that there should be one consistent definition of security incident across these rules - CERT-In rules, sec43A (all Rules), RBI guidelines etc.**

- Rule 2 (h) e-PPI Issuer - the definition needs to clearly state whether it will only apply to entities regulated / licensed under the PSS Act.

- Rule 2 (j) Multi-factor authentication: The factors used for the purpose of implementing multi-factor authentication should be determined by the e-PPI Issuer and not specified by the Central Government. This is in-line with the flexibility provided to banks by RBI. The manner of authentication of customers is evolving with time through newer and better technologies. Government should not specify factors for multi-factor authentication, as this will make it difficult to upgrade to the latest technology, which may be more secure and achieve the intended result. For instance, some entities use a PIN, most banks are using OTP, certain player's have evolved to use biometrics and now certain banks and Visa/ Mastercard checkouts are evolving to use device authentication as a second level authentication. Therefore, in order to ensure that the intended result is achieved, while not curbing innovation, we propose modification to the definition as follows: *authentication based on the use of two or more elements categorized as knowledge, possession and/or inherence, as determined by the e-PPI Issuer*".

3. Information Security Policy

- Rule 8 in **Sec 43A rules regarding 'Reasonable Security Practices and Procedures' already requires Body Corporates (which covers ePPIs) to have an information security policy in place**. We feel, there is no need to define new requirements under these rules.

4. Privacy Policy

- Rule 4 of the sec 43A rules already lays out the requirement for defining a privacy policy. Hence there is no need to specifically have this clause. Further, rule 4 **should not include the need to publish period of data retention** which is the right approach as it is not practical to state the period in the policy.

- It is not clear how does *"Sharing of Information with Law Enforcement Agencies" needs to be included in the Privacy Policy*

- With respect to the rule requiring the privacy policy to include the "name and contact" of the Grievance Redressal officer - this is not a practical requirement as many times companies deploy teams to monitor and address grievances. In fact, we would suggest MeitY to also accept this suggestion for the existing Grievance Redressal requirements for Reasonable Security Practices and Procedures Rules in the IT Act.

5. Risk Assessment and Risk Control

- The manner and timelines in which PPI issuers are required to carry out review of security measures and risk controls, the annual audit by auditors empanelled by the Indian Computer Emergency Response Team (CERT-In) and the coverage of the audit has already been defined by RBI through the Payment and Settlement Regulations, 2008 and **RBI notifications including notification on Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers** dated December 9, 2016.

- In addition, the notification indicates the particular areas of security requirements while giving the flexibility to PPI Issuers to determine the security measures dynamically depending upon the emerging risks. We are supportive of this approach.

6. Customer Identification & Authentication

- One of the primary use cases for e-PPIs arise from the fact that e-PPI transactions are seamless and do not require multi-factor authentication. **Low value transactions should continue to operate in a similar manner.**

- A use case wherein a Customer uses his/her Credit/ debit card to load the wallet after completing a second level authentication. Thereafter the customer makes a transaction using his/her e-PPI and once again has to go through a multi-factor authentication. **Why would the customer opt to use his/her wallet over making a direct transaction using his/her card or net-banking account esp. considering that customers don't get interest paid when using PPIs**. Especially after the launch of Unified Payment Interface, such rules on e-PPI will completely limit the

use of e-PPI.

- Use cases such as payment wallet integrated with the taxi aggregator services does not require customer two factor credentials to initiate the payment against a value stored in ePPI.

- With continuous advancement of technology, additional factor authentication is not the only way to ensure security & prevent fraud. There are measures like **Device ID checks (using Near Field Communication/ Wireless Application Protocol), IMSI/MSISDN checks, Velocity Limits, Tokenisation, Location** & many more ways that ensure much **better level of security** without compromising on customer convenience.

- The **authentication parameters should not be obligated by the Government**. **It should be left to individual players to put in place a mechanism to ensure security of transactions.** Technology evolution and competition among players will ensure that adequate authentication measures are put in place.

- Additional factor of authentication should be relevant only when payment is happening on a third party merchant. In other cases, where money is moving within the ecosystem of an entity, additional authentication requirements should not be required. Even in third party payments, we think that individual players should have the freedom to build right authentication mechanisms as per specific transaction type, amount, customer profile, and past customer history.

- Rule 6 (5) (d) & (e) are unreasonably stated. What is required is implementation of adequate velocity checks and risk mitigation measures to try to prevent unauthorized access (at any point) and fraud. Rather than requiring ePPIs to 'protect manipulation by third parties" or "prevent, detect and block fraudulent payments before the e-PPI Issuer's final authorization", the rule should be reworded to require e-PPIs to implement appropriate velocity checks and risk mitigation measures that attempt to help in preventing, detecting and blocking unauthorized access to payment systems (including during authentication procedure) or fraudulent payments.

7. Personal Information

- The **term "information collected" used in the rules is too broad and could include non-Personal Information as well**. It needs to be made consistent with the definition of PI already defined in section 43A rules - "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person (i.e., Personally Identifiable Information).

- Also, there should be **regulatory level playing field between e-PPIs and other players dealing with financial information**; and no additional compliance burden (by treating all aspects of transaction history as sensitive personal data for

ePPIs) should be placed on e-PPIs.

8. Security of Personal Information

- Given that **section 43A Rules are applicable for Sensitive Personal Data or Information and does not extend to personal information**, including Section 72A requirements in 43A rules might be legally incorrect as 72A talks about punishment for disclosure of personal information in breach of a lawful contract.

- Rule 8 of the Sec43A already defines reasonable security practices which are applicable to e-PPIs and there appears no need to specify new requirements. **Are Security requirements for PI different for Security requirements for SPDI under these Rules?** It might lead to confusion. Further, RBI PPI guidelines already define security requirements for e-PPIs.

- On Rule 8 (2) the requirement for e-PPIs to ensure that merchants contractually comply, Rule 7 of the sec 43A rules already specific such requirements and there is no need for new requirements. Rule 8(2) must not apply retrospectively and reasonable timeframe should be provided to e-PPIs to review contracts.

9. Access to Personal Information

- The **Sec 43A rules already include the access and disclosure requirements which are applicable to e-PPIs.**

- This is too restrictive and only allows access to personal information with consent. The provision **should carve out legitimate exceptions** (sharing without consent) like when disclosure is required to fulfil legal requirements, provide technical & user support and other business obligations and requirements.

10. Reasonable Security Practices to be applicable

- The requirements specified become applicable **by virtue of ePPI being Body Corporate** under the requirements of Rule 8 of sec 43A rules

11. End-to-end encryption

- **The rules should not make end to end encryption mandatory.** The deployment of encryption is subject to various considerations such as security needs, product design, compatibility, performance, costs versus risk analysis, etc. **Taking a 'one size fits all' approach will not work** - the policy needs to provide flexibility to businesses to deploy encryption based on their specific needs, while achieving the intended result. For example, E2E encryption of only credentials combined with adequate velocity checks and risk mitigation measures, may achieve the intended

result.

- In addition, the rules **do not clarify if, E2E encryption is required with respect an e-PPI transaction carried out by the customer or does it extend to loading of the prepaid payment instrument**. In case E2E encryption is required with respect to loading transactions, the Rule will not only require implementation by the e-PPI Issuer and the respective merchants but would involve other industry members such as Acquiring Bank, Card Associations, issuing Banks. Such an approach will not be practically possible.

12. Traceability

- Clarity is sought on what is meant **by 'all interactions with customers and other service providers in relation to accessing payment accounts or initiating payments"**. The term 'all interaction' is very wide and can include customer service requests or notification sent with respect to the payment account or logging in the e-PPI account without any further activity. In might not be practical to maintain all interactions, as there is also cost involved, and especially in case of startups, it might be a significant cost.

- The information required **should be limited to the transaction logs and customer/service provider due diligence documents and information**. Language should be modified accordingly.

- Further, "**initiating transaction" is also wide and will include all attempted yet incomplete transactions**. Clarity is sought when is a transaction deemed to be initiated for the purpose of this rule? For instance, are records of all bounced, rejected, failed, abandoned transactions required to be maintained? In addition, will a transaction that fails to be concluded for technical reasons like loss of connectivity, be also deemed to be 'initiated'?

- In the event that all **interactions include any and all communication between the e-PPI Issuer and the Customer or Service Provider**; clarity is sought on the time period for which such information needs to be retained, consistent with the retention periods that may have been prescribed for similar transactions or information through legislative enactments or through guidelines issued by sectoral regulators like the RBI.

13. Retention of information

- This **section is too restrictive in allowing data retention** only for the periods **as specified by the Central Government**. e-PPIs need to retain data for other legitimate business requirements and obligations including for legal reasons. The term 'only' is not acceptable. Further, different classes of records have different retention requirements. Regulators specify different requirements on Data retention and storage – eg TRAI, RBI

- Further, the Prevention of Money Laundering Act and RBI guidelines made thereunder already provides the data required and timelines for maintaining identifiable and transactional data[1]. Considering that the type of data and timelines for retention for the purpose of identifying the customer/service provider and transactions that have been attempted or executed have been detailed out by a statute and RBI, having parallel rules is not practical.

- The data retention requirements should abide by the principles of transparency, proportionality, accountability, due process and limits on data to safeguard privacy and minimize costs esp. from Startups viewpoint.

14. Reporting of cyber incidents

- **DSCI-NASSCOM support standardization and maturity in information exchange and incident reporting as the increasing trend of cyber-attacks requires a community-based approach.** Alignment between various government agencies to ensure the reporting requirements are consistent and easy to follow will be key to successful implementation and wide adoption of this effort. From industry viewpoint, **if requirements for multiple reporting can be harmonized, it will be very helpful to avoid duplication of efforts.** Hence it is imperative to construct a harmonized security incident or breach reporting model for financial ecosystem in India, which can minimize the industry efforts leading to optimization of resources.

- Also, government should further classify the criteria based on which company can easily determine which incident to report. ***The types of incident and reporting requirements should be concretely defined so that the compliance remains meaningful and only relevant incidents are reported.***

15. Customer awareness and education

- The awareness section seems very prescriptive. The section should talk about raising security awareness on the PPI technologies and its processes, and in consultation with the regulators, these should be formulated.

16. Grievance redressal

- We understand that an adequate complaint redressal system is a necessary and the details regarding the process and the contact details should be mentioned on the website. However, RBI guidelines on PPI already address the grievance

[1] Prevention of Money-Laundering Act, 2002 ("**PMLA**"), the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 ("**MR Rules**") and the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016 ("**Master Directions**").

redressal process - The non-bank PPI issuer shall put in place an effective mechanism for redressal of customer complaints along with escalation matrix and publicize the same for the benefit of customers. RBI further requires a 16/7 customer support to be in place by e-PPI Issuers and lays down a process for e-PPI Issuers to report customer complaints to RBI.

- In case of prepaid payment instruments issued by banks, customers shall have recourse to Banking Ombudsman Scheme for grievance redressal. Further, in case of breach of SPDI, the rules made under Section 43A of the IT Act already provide for a Grievance redressal.

- Wrt rule requiring publishing of "name and contact" of the Grievance Redressal officer - this is not a practical requirement as many times companies deploy teams to monitor and address grievances. In fact, we would suggest MeitY to also accept this suggestion for existing Grievance Redressal requirements in Sec 43A Rule 5(9) of ITAA, 2008

- Timeline for Grievance officer to act upon request needs to be increased to 72 hours and one month of resolution time should be defined from the point the customer has provided all the requisite details required to resolve the query. We also need to take cognizance of the fact that timely resolution maybe dependent on external entities such as banks, payment gateways etc.

- Hence, there is no need to specify any new requirements specifically for e-PPIs.

17. Security standards

- There is no need to define new security standards for e-PPIs for the following reasons:
    - RBI's PPI guidelines already include requirements to deploy appropriate security measures: *The pre-paid payment instrument issuers shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds. It is necessary to have a centralized database/ MIS by the issuer to prevent multiple purchase of payment instruments at different locations, leading to circumvention of limits, if any, prescribed for such payment instruments.*
    - There is also RBI notifications including notification on Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers dated December 9, 2016
    - Rule 8 of the Sec43A rules defines requirements for 'reasonable security practices' providing ISO 27001 as a reference
    - Security concerns can be best addressed through voluntary adoption of cyber security standards and best practices by e-PPIs. The cyber

threat landscape is ever evolving and regulatory prescriptions will only drive companies towards compliance instead of addressing such evolving threats. Various industry standards for security are already available and many are evolving. Competition and brand reputation are significant drivers for e-PPIs to invest in security. Hence, government should only specify security requirements at a very high level and should not prescribe specific standards or detailed requirements.

- To the extent possible, international standards should be followed. Only if there is a consensus that global standards do not address specific security requirements should a local standard be considered. When considering development of a security standard, the government should follow a consultative process, where the industry works with the government to define such standards. The government should incentivize and encourage the industry to adopt standards rather than prescribe them.