भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2016-17/178
DPSS.CO.OSD.No.1485/06.08.005/2016-17 December 09, 2016

All Prepaid Payment Instrument Issuers,
System Providers, System Participants and
all other Prospective Prepaid Payment Instrument Issuers

Dear Sir,

Security and Risk Mitigation measure - Technical Audit of Prepaid Payment Instrument issuers

With the withdrawal of legal tender characteristics of existing ₹ 500/- and ₹ 1000/- Bank Notes (Specified Bank Notes – SBN), the use of alternate modes of payment, specifically e-wallets has gained momentum. The Reserve Bank has also notified special measures for Prepaid Payment Instruments (PPIs) to facilitate adoption of digital payments in a big way. While all efforts should continue to be made by entities for on-boarding new customers and merchants, it needs to be borne in mind that any kind of cyber security incident affecting the digital channels/products, particularly at this juncture, may have significant system-wide ramifications and act as a dampener for the adoption of digital products by public at large.

2. As the rapid escalation in e-payments may put significant pressure on the existing digital infrastructure, it is imperative that the integrity of our digital ecosystem is maintained by ensuring that they remain robust and fully secure. Attention is drawn to the extant guidelines requiring authorised entities to submit system audit reports from a CISA/DISA qualified auditor on an annual basis (refer the links https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=6177&fn=9&Mode=0 and https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=6344&fn=9&Mode=0). The scope of the System Audit includes evaluation of the hardware structure, operating systems and critical applications, security and controls in place, including access controls on key

applications, disaster recovery plans, training of personnel managing the systems and applications, documentation, etc.

3. In view of the above, all authorised entities/banks issuing PPIs in the country are advised to:

i. carry out a special audit by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In) on a priority basis and take immediate steps thereafter to comply with the findings of the audit report. The list of empanelled auditors is available on http://www.cert-in.org.in/PDF/Empanel_org.pdf The audit should cover compliance as per security best practices, specifically the application security lifecycle and patch/vulnerability and change management aspects for the system authorised and adherence to the process flow approved by the Reserve Bank. Banks may also be guided by the circular DBS.CO/CSITE/BC.11/33.01.001/2015-16 on Cyber Security Framework in Banks dated June 02, 2016.

ii. take appropriate measures on mitigating phishing attacks considering that the new customers are likely to be first time users of the digital channels. Safety and security best practices may be disseminated to the customers periodically.

iii. implement additional measures dynamically depending upon the risk perception or threats as they emerge.

4. A confirmation giving the details of action plan, including the name and date of appointment of the auditor may please be conveyed to Department of Payment and Settlement System DPSS, CO at email by December 21, 2016. Also, a senior functionary may be designated to monitor the position on an ongoing basis and report the updates to us periodically (1st compliance within 15 days and subsequent compliance on a monthly basis). Banks may forward the compliance to the respective Senior Supervisory Manager (SSM) and non- bank entities may forward to the respective regional offices of DPSS.

5. The directive is issued under Section 10(2) read with Section 18 of Payment and Settlement Systems Act 2007, (Act 51 of 2007).

Yours faithfully,

(Nanda S. Dave)
Chief General Manager