

NPCI/2018-19/RMD/009

18th September 2018

To,
All Members of National Financial Switch (NFS) / RuPay,

Dear Sir / Madam,

Subject: MACing of Card based Transactions routed through NPCI

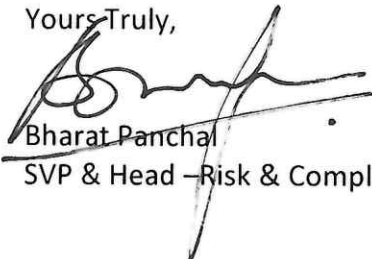
Considering the rising threat of cyber-attacks on payments infrastructure, it is necessary that Banks and their ASPs (where applicable) enhance their security systems to counter the ever increasing threat of potential cyber-attacks. NPCI deems it absolutely vital for Banks to take appropriate measures for enhancing the security of the transactions routed between the Bank / ASP Switch and NPCI Switch.

As one of the preventive measure to ensure the integrity / nonrepudiation of the message, MACing has been decided to implement between NFS / RuPay switch and member bank's switch. In proposed MACing, Message Authentication Code errors or MACing errors in Banking transactions pertain to a Message Authentication Code which is a "token" that can be included within a transaction message as it emanates and returns back to an ATM / POS terminal. Real-time notification of MAC errors is proven to improve problem isolation, and decrease the number of reported incidents for lost communications which can consequently improve transaction security in the payments ecosystem.

In this regard, vide this circular we advise your Bank to carry out necessary changes in your Switch as per the attached guidelines. Banks with their in-house switching system are advised to implement MACing by 30th November 2018. For Banks supported by ASPs, kindly advise your ASPs to adhere the deadlines notified by NPCI via separate circular.

Should you require any help for enabling MACing for your Bank Switch, we request you to get in touch with your ASP or assigned NPCI Relationship Manager.

Yours Truly,



Bharat Panchal
SVP & Head – Risk & Compliance Officer

encs: Guidelines on MACing