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

RBI / 2012 -13/424
DPSS (CO) PD No.1462 / 02.14.003 / 2012-13 February 28, 2013

The Chairman and Managing Director / Chief Executive Officers
All Scheduled Commercial Banks including RRBs / Urban Co-operative Banks /
State Co-operative Banks / District Central Co-operative Banks/
Authorised Card Payment Networks

Madam / Dear Sir,

Security and Risk Mitigation Measures for Electronic Payment Transactions

Payments effected through alternate payment products/channels are becoming popular among the customers with more and more banks providing such facilities to their customers. While this move of the banks indeed promotes and encourages the usage of electronic payments, it is imperative that the banks ensure that transactions effected through such channels are safe and secure and not easily amenable to fraudulent usage. One such initiative by RBI, was mandating additional factor of authentication for all card not present (CNP) transactions. Security of card present transactions has also been initiated by RBI through the implementation of recommendations of the Working Group on Securing Card Present transactions. Banks have also put in place mechanisms and validation checks for facilitating on-line funds transfer, such as: (i) enrolling customer for internet/mobile banking; (ii) addition of beneficiary by the customer; (iii) velocity checks on transactions, etc.

2. With cyber-attacks becoming more unpredictable and electronic payment systems becoming vulnerable to new types of misuse, it is imperative that banks introduce certain minimum checks and balances to minimise the impact of such attacks and to arrest/minimise the damage. Accordingly, banks are required to put in place security and risk control measures as detailed here under:

A. Securing Card Payment Transactions

(i) All new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customer. Such cards enabling international usage will have to be essentially EMV Chip and Pin enabled. (**By June 30, 2013**)

(ii) Issuing banks should convert all existing MagStripe cards to EMV Chip card for all customers who have used their cards internationally at least once (for/through e-commerce/ATM/POS) (**By June 30, 2013**)

(iii) All the active Magstripe international cards issued by banks should have threshold limit for international usage. The threshold should be determined by the banks based on the risk profile of the customer and accepted by the customer (**By June 30, 2013**). Till

such time this process is completed an omnibus threshold limit (say, not exceeding USD 500) as determined by each bank may be put in place for all debit cards and all credit cards that have not been used for international transactions in the past.

(iv) Banks should ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry- Data Security Standards) and PA-DSS (Payment Applications -Data Security Standards) (**By June 30, 2013**).

(v) Bank should frame rules based on the transaction pattern of the usage of cards by the customers in coordination with the authorized card payment networks for arresting fraud. This would act as a fraud prevention measure (**By June 30, 2013**).

(vi) Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS certification. This should include acquirers, processors / aggregators and large merchants (**By June 30, 2013**).

(vii) Banks should move towards real time fraud monitoring system at the earliest.

(viii) Banks should provide easier methods (like SMS) for the customer to block his card and get a confirmation to that effect after blocking the card.

(ix) Banks should move towards a system that facilitates implementation of additional factor of authentication for cards issued in India and used internationally (transactions acquired by banks located abroad).

(x) Banks should build in a system of call referral[1] in co-ordination with the card payment networks based on the rules framed at (v) above.

B. Securing Electronic Payment Transactions

The electronic modes of payment like RTGS, NEFT and IMPS have emerged as channel agnostic modes of funds transfer. These have picked up to a large extent through the internet banking channel and hence it is imperative that such delivery channels are also safe and secure. Some of the additional measures that need to be introduced by the banks could be as follows:

(i) Customer induced options may be provided for fixing a cap on the value / mode of transactions/beneficiaries. In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon.

---

1 Call Referral implies:-
-Card is swiped at the EDC at the merchant.
-Issuer responds with a "Call Issuer" decision.
-Merchant calls the acquiring bank with details of the card number and transaction data.
-Acquirer calls the issuing bank to seek authorization
-Issuing bank approves/ declines the transaction post speaking with the customer and validating the transaction.
-Merchant will need to swipe the card again to obtain approval

(ii) Limit on the number of beneficiaries that may be added in a day per account could be considered.

(iii) A system of alert may be introduced when a beneficiary is added.

(iv) Banks may put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.

(iv) Introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered.

(vi) The banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions.

(vii) Capturing of Internet Protocol (IP) address as an additional validation check should be considered.

(vii) Sub-membership of banks to the centralised payment systems has made it possible for the customers of such sub-members to reap the benefits of the same. Banks accepting sub-members should ensure that the security measures put in place by the sub members are on par with the standards followed by them so as to ensure the safety and mitigate the reputation risk.

(viii) Banks may explore the feasibility of implementing new technologies like adaptive authentication, etc. for fraud detection.

The above security measures under B (i) to (viii) are expected to be put in place by banks by June 30, 2013.

3. Banks are advised to quickly implement the above security/risk mitigation measures and keep us posted with the progress made in this regard.

4. The directive is issued under section 18 of Payment and Settlement Systems Act 2007, (Act 51 of 2007).

5. Please acknowledge the receipt of this circular.

Yours faithfully,

(Vijay Chugh)
Chief General Manager

Related Press Release	
Feb 28, 2012	RBI releases Security and Risk Mitigation measures for Electronic Payment Transactions