Workshop on Card Frauds organised by NIBM, Pune

Topic: Security Issues in Card Payment System – Are we on right track?

- *By A P Hota*

Ladies and Gentlemen, Good Morning!

At the outset, I express my sincere gratitude to National Institute of Bank Management (NIBM), Pune and Mr Allen C Pereira, Director in particular, for conceiving the idea of this Workshop which is so topical and relevant and requesting me to speak at the opening session. The increasing incidents of frauds in the cards payment system, both in terms of volume and value, modalities for carrying out the transactions, instances of wider and deeper trails from origin of data compromise to points of fraudulent use in varying geographies have brought to focus the need for all stake holders to work together. The issue is exercising the attention of all and more particularly the regulators from the angle of payment systems regulation and supervision. I am told that the workshop has participants from various interest groups – card payments professionals from banks, solution providers, processors and government agencies dealing with cyber-crime and Reserve Bank of India, the regulator. This is a perfect setting for holding the workshop and I congratulate Mr. Pereira and his Team.

In my opening remarks, I would cover three broad aspects of the security issues in Card Payment Systems in India.

The first logical question is how big is card payments market in India?

This can be answered by a few statistical indicators -
336 million debit cards, 19 million credit cards, 1,20,000 ATMs, nearly 9,00,000 POS terminals, 18 prepaid service providers authorised by RBI, transaction level of 45 million debit card transactions for Rs 7,000 crores in value per month and 31 million credit cards transactions for Rs 12,000 crore in value per month shows that the card payment industry is no longer small as it used to be 5 years back. The hallmark of a mature industry is the co-existence and growth of all types of specialist institutions relating to card payment ecosystem- competing and thriving. Good news is that very few instances of failing. The specialist institutions can be card payment networks like VISA, MasterCard, Amex, and the emergent RuPay domestic network, switch solution providers like ACI, FIS, Euronet, Postilion, OPUS, YCS and Infrasoft, specialist companies like FirstData, Global Payments, Atos Origin and BankNet in transaction acquiring space apart from big acquiring banks like HDFC bank, Axis Bank and State Bank of India, Card Management solution companies like TSys, FSS and YCS, Reconciliation companies like In Solutions Global, Risk Solution companies like Arcot and Paladion, Certification agencies like Silicomp India, Online payment Gateway companies like Enstage, FSS, Arcot and OPUS and Merchant Aggregators of very big size like Billdesk and Tech Process. There are many other specialist institutions in ATM Deployment like Prizm Payments and Cash-In Transit companies like CMS and Brincs Arya, analytics companies like FICO and Alaric and various consulting organisations. In short, the card payment market in India is now at takeoff stage. Small start-up companies like Transaction Analysts with about 10-15 staff members are also operating profitably. In my interactions with the Private Equity funds, I notice that enormous investments are being made on payment processing companies. An analysis reveals that cash withdrawal at the 1,20,000 ATMs in the country is as high as Rs.7000 crore a day.

In sum, the size of the card payments market in India is big and getting bigger each day.

The second logical question is what the incidence level of card frauds in India is and whether it is alarming?

Unfortunately, statistical compilation of incidences of card fraud is an area which is still in nascent stage. Reliable data is not available in public domain the way we can access payment system data at Reserve Bank's website. Card scheme companies also do not publish data – partly due to ownership of data and partly due to the challenges in collection and compilation.

Unlike our counterparts in the United States, the United Kingdom and other developed economies where the frauds are reported as part of the legal and regulatory mandate, in India, regrettably, there is no legislation to make frauds available in the public domain. The focus of Financial Intelligence Unit (FIU) is money laundering and not fraud per se. Neither banks, are legally mandated to report frauds though they are required to file regulatory returns to RBI for frauds exceeding a cut-off limit. Thus comprehensive data is not available anywhere.

In February 2013, an interesting report had appeared in Times of India, Mumbai. The annual crime statistics on the Mumbai police website showed single-digit figures and some low double-digit ones in the city's cyber crime list for the past three years. Only 47 cases of credit card frauds and 17 phishing cases were noted from 2010 to 2012. The reporter had amusingly cited the observations that 90 police stations in the city *(besides the cyber crime cell and the cyber police)* receive at least 150 complaints a day about banking frauds, hacking, phishing or other credit card misuses. Thus, card fraud incidents are still anecdotal and yet to get statistical. It would be ideal if the incident statistics get published in RBI Bulletin at monthly rest in the public domain the way various other card payment statistics are published.

However, there is some data available. During February 2013 in the Indian Parliament, Minister of State for Finance reported 8322 positive cases of fraud related to cards and internet banking during calendar year 2012 involving ₹ 53 crore. As per another source, the number of cyber frauds which used to be around 14,000 for Rs. 40 crore in 2010-11 went up in value terms to Rs. 67 crore in 2012-13, though in terms of number, it came down to 8700. In sum, I would state that reliable data is not available.

Even in the absence of reliable statistics, I can speak with my experience that the number of card fraud has been rising. In our experience of running the NFS network for ATM transactions, we have experienced several instances of ATM card fraud. Last year NPCI had constituted a Task Force on ATM Security and had compiled interesting cases of ATM frauds listing the instances of modus operandi. The Task Force had made several recommendations of preventive steps to be taken by banks. One such recommendation was disablement of cash retraction. The Report explained at length the modus of card skimming, card raiding, robbery etc. In a very recent incident, fraudsters used skimming device inside the card slot of ATM devices to capture the information of cards and to make fake cards to commit the frauds.

In the world of on-line cyber-crime, there are organised groups for sourcing data in one geography and carrying on the transactions in another. Use of payment cards acceptable in all parts of the globe in the globally interconnected payment system – which is so typical of card payment system- has made cyber crime easier. As per the Symantec Internet security Threat Report 2013, countries leading the charts are United States, China and India, and India accounting for 6.5% of the total targeted attacks in 2012.

In sum, the incident level, though not alarming, is a matter of concern. Since several countries have taken several preventive steps, we should guard ourselves against card fraud moving to India.

The third and important question is what all steps have been taken by Reserve Bank in the recent past to address the issues of card frauds.

My short answer to this question is that Reserve Bank of India has done significant amount of work on this issue since 2009. I will narrate a few such regulatory measures which will give a sense to what extent the regulator is keenly observing the card payments market and in some cases leading the world.

The ***first*** major direction came in 2009 to put in place a system for additional authentication / validation based on information not visible on the cards for on-line card not present transactions. It was effective from August 1, 2009. Subsequently, it covered the IVR/ MOTO and recurring transactions as well. Initial reaction in the market was one of sudden decline in the volume of transactions. This measure was primarily aimed at preventing fraudulent use of stolen cards or stolen card data. It was a step ahead of the developed world and many countries are now emulating India. Once the online merchants – mostly the airline ticketing industry adjusted themselves to the new regime and the customer confidence on security improved, card present transactions also got a fillip. IRCTC is now the largest online merchant in the country registering around 5,00,000-plus transactions a day. Additional factor authentication for on-line transactions in India is now a much talked about success story in cards payment.

The ***second*** regulatory measure of stipulating “online alerts” to the card holder for all card not present transactions for value of Rs 5000 and above is another security measure that has provided a lot of confidence to the customers. Banks, on their own have started sending

alerts for all card transactions irrespective of amount and irrespective of whether it is card present or card not present transaction. By the time the transaction slip is printed and given to customer for signing, mobile alert is already available. This has a salutary effect on preventing card fraud. Timely action on many incidents of card fraud could be taken by customers primarily because of on-line alerts. Customer can issue de-activation request as soon as an alert is received for transaction not done by the customer.

The ***third*** and most important regulatory measure was to create the infrastructure readiness for migration to EMV Chip and PIN cards. Based on a Working Group recommendation and wide consultative process, Reserve Bank stipulated 30th June 2013 *(just three weeks away)* for all issuing banks to get ready from technical perspective to issue EMV cards. 30th June 2013 is also the deadline for commercial readiness of acquiring infrastructure to support PIN at POS transactions. POS infrastructure has also to be readied for accepting EMV Chip cards. The purpose behind this regulatory measure was to make POS based transactions as secure as the ATM transactions where an additional authentication of PIN is necessary. A majority of cards issued in India are magnetic -stripe cards and data stored on such cards are vulnerable to skimming and cloning. It is gathered that most of the large banks are ready for migration for use of PIN at POS transactions from 30th June 2013.

The ***fourth*** measure pertains to mandating the use of EMV Chip card and PIN to be issued to customers who have evidenced at least one purchase using their debit/ credit card in a foreign location. To me, this measure would have a salutary effect. Currently, card issuing banks prefer to issue International debit cards with the assumption that multi-function card can lead to savings not realising the enhanced fraud exposure. It is gathered from various informal discussions with banks that only about 5 percent of debit card holders and about 10 percent of credit card holders use their cards abroad. Many international card holders still prefer to carry foreign exchange travellers' cheque or cash while travelling abroad. The popularity of Forex Pre-paid card has in fact made international debit card irrelevant. Therefore, it makes logical for the regulator to stipulate that all new debit and credit cards to be issued only for domestic use unless international use is specifically sought by the customer.

The **fifth** measure pertains to adoption of Payments Cards Industry Data Security Standards (PCIDSS) by 30th June 2013. Banks have been advised that the terminals installed at the merchants for capturing card payments *(including the double swipe terminals used)* should be PCI-DSS and PA-DSS compliant. Though the recent incidents of data compromise have

taken place at installations which were already PCI-DSS compliant, the importance of adoption of PCI-DD / PA-DSS standards cannot be minimized.

The **sixth** and the last pertain to move towards real time fraud monitoring system at the earliest. For this, I am aware banks are gearing themselves fully. NPCI has provided real time fraud monitoring solution to all the National Financial Switch (NFS) member banks.

Concluding thoughts

For my concluding thoughts, I will refer to the title of my opening remarks : Security issues in Card Payment system in India – whether we are on the right track?

My reply is an emphatic 'Yes'. But, considering the rapid growth of the cards payment market, sooner we adopt additional factor of authentication for card present transactions at POS terminals (needless to mention that they are to be PCI-DSS/ PA-DAA compliant), the better. Banks have been undergoing a painful compliance process. But, it is worth. The debate as to whether the country should go for EMV Chip and PIN or Aadhaar based authentication is actually not a debate. It cannot be settled by an answer in either or. Aadhaar is in an evolving stage and a Working Group appointed by Reserve Bank of India is looking at it. On a long term, Aadhaar makes sense. But, we cannot wait for entire Aadhaar infrastructure to be ready for the entire market. The card payments market is so big that even if EMV Chip and PIN is adopted for international cards now, a much bigger market for Aadhaar authentication still remains. We may need Aadhaar for one market, EMV Chip & PIN for another and NFC contactless for yet another. Fraudsters are a step ahead of market and innovators in one sense. We all card professionals need to stay vigilant.

I once again congratulate NIBM's efforts in holding the workshop on a subject critical and topical and inviting me to deliver the opening remarks.

I thank you all for your kind attention and patient hearing. Please have a great day.

Inaugural address delivered by Shri. Abhaya Prasad Hota, MD & CEO, National Payments Corporation of India at the Workshop on Card Fraud organised by NIBM, Pune on June 07, 2013 at Mumbai Cricket Association, Mumbai. The speaker acknowledges the contributions of Shri. Abhishek Nayak and Shri. Suresh Shenoi of the National Payments Corporation of India.

****