G Padmanabhan: Secured online banking vs. customer convenience – opportunities and challenges

Comments by Mr G Padmanabhan, Executive Director of the Reserve Bank of India, at the Annual Conference on Secure Banking 2011, Mumbai, 29 July 2011.

* * *

Assistance provided by Shri K. Sivaraman and Shri P.K. Chophla in preparation of these comments is gratefully acknowledged.

Ladies and Gentlemen,

Good morning.

It is my pleasure to be here amongst all of you in the Annual conference on secure banking 2011, and share with you some of my thoughts on the subject. I thank IBA and MP TFCI, co-organizers for the event, for this opportunity.

Banking, as all of us know, is a business activity synonymous with Trust, and security in banking is a paramount presumption for trust. The concept and perception of such security in banking has, over a period of time, changed drastically, in tandem with changes in the way banking business is conducted. Assets with the banks are maintained more in digitized rather than physical form, transactions are carried out over technology enabled platforms/applications and communications are over electronic modes. Physical, Geographical and "product" boundaries are no more the constraints for the growth of banking business, which is rapidly expanding. There are newer products and channels of delivery. Networked environment has enabled delivery of banking services at the doorstep of the customer. Anywhere anytime banking with core banking and newer delivery channels viz., ATM, online banking, mobile banking etc. have provided convenience of banking to the customer and an increasing number of people rely upon the convenience and ease of use of Internet banking services in their business as well as daily life. But, this also enhances customer expectations about efficient delivery with security. Retaining customer loyalty and thus, business in a fiercely competitive electronic banking industry lies in delivering customer expectations.

In the IT enabled banking environment, it has to be recognized that fraud possibilities have assumed international dimensions. As it is often said, in a chain, it is the weakest link that is most vulnerable. Therefore, it is not only important to *ab initio* set up a safe platform, one needs to make sure that the so called "Safety" is continuously benchmarked against international standards. In such a scenario, all the three attributes of information security viz. confidentiality, Integrity and availability at all the relevant stages of entry, storage, and transaction acquire immense importance. As such, there has to be a paradigm shift in the perception about security in banking and responses to the same.

The threats which bother every one of us in the context are multifold, ranging from password hacking, card copying/cloning to data and identity theft at various levels of transaction, information storage as well as transmission stage. Managing security is more challenging in online and phone banking as compared to other delivery channels. Online threats in the form of phishing attacks, spyware, viruses, Trojans, key loggers are frequent. Threats from ATM take the form of ATM skimming, eavesdropping, spoofing, service denial, etc. Identity theft in the electronic transactions is a growing cyber crime. Innovative methods of hacking and stealing come to the fore regularly and the industry has to take prompt action to safeguard business and customer interest.

As per information published by CSIS (Center for Strategic and International Studies, US), between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised. As of

April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million. I am flagging this issue to highlight the point that hackers have started to target medium and small organisations given the increasing safety standards put in place by large organisations. Further they shift geographical locations targeting vulnerable jurisdictions with lax security.

Apart from the above, lack of customer awareness itself is an important concern, which aggravates threats to security. According to the findings of a survey, conducted by DSCI and KPMG in the year 2010, on the state of data security and privacy in Indian banking, "One of the most significant information security challenges highlighted by the banks in the survey is lack of customer awareness on information security and the threat from insecure customer end points. The boundary-less cyberspace exposes the banks to internationally organized crimes and new age threats. Further, with banks increasingly working with third parties and in the process, sharing business information, management of third party risks is also becoming a challenging task'.

Let me amplify with a few examples on what I have been saying so far.

You are aware that the Reserve Bank of India introduced the system of a Second Factor of Authentication for all Card Not Present transactions almost two years back. This measure has ensured greater security in online card transactions and instances of online frauds has considerably dropped. More importantly, this has resulted in a significant growth in card transactions in this mode reflecting the enhanced level of customer confidence. Perhaps as a consequence, the focus of fraudsters has shifted to card present transactions. For example, in Chandigarh, card data – including the PIN - was compromised at a few ATMs. The stolen information was used to clone the cards to withdraw cash from various locations across the country. There was certainly a breach of security at the ATMs where the data was compromised. It is important that bankers need to ponder on how to tackle this issue through technology.

On its part, the Reserve Bank has mandated with effect from July 01, 2011, a system of alerts for all card transactions, irrespective of the channel used. Such a system will surely help in containing frauds. However, it is for the banks to make this effective by ensuring that the customers are persuaded to register their mobile phone numbers for receiving the alerts.

Fraudsters are not only tech savvy but have clear understanding of the systems and procedures obtaining in banks. There have reportedly been instances in Coimbatore where PoS terminals were set up after due compliance with the KYC requirements and stolen cards were used to transact at these terminals by the fraudsters. (I believe that the fraudsters used stolen card details purchased through online e-payment schemes operating internationally to acquire such information)

In Hyderabad, fraudsters posing as merchants offered Baskin Robbins/mobile recharge voucher talk time worth Rs.250 against payment of a mere Rs.50. The condition being only debit cards would be accepted. The kiosk machine set up was configured to prompt for PIN and print a charge slip indicating approval of the transaction by the Bank. The Magnetic Stripe Card data and the PIN were captured from the unsuspecting customers and later used to make counterfeit cards for withdrawal of cash. The typical customer response to such incidents was "But it is the primary responsibility of banks to ensure safety of my money. They cannot leave it to customers". The same modus operandi was used at a Petrol Pump in Ranchi; only this time instead of mobile recharge voucher, customers were offered car wash liquid and air freshener. Bankers may argue that there was no breach of security of their systems and these were driven by the customers' avarice. While conceding this point, the purpose of my citing these instances was to highlight the need to constantly educate customers. With banks encouraging customers to move more and more towards electronic modes of payments, it is necessary to realize that however robust and secure the systems deployed may be, it is the customers' perception that matters in the end.

It may not be out of place to mention that the Reserve Bank of India recently commissioned a survey of the customer service obtaining at various ATMs across the country. While the overall satisfaction with the usage at ATM at the national level was found to be at 7.8 on a scale of 1-10, it was well below the national average in states like Uttar Pradesh, Gujarat and Chandigarh. However, the survey revealed scope for improvement in the grievance redressal mechanism. Over two third of the respondents revealed that they had noticed the help-line number at the ATMs. Over 52% of the respondents reported that complaint resolution took about two weeks or more. But what is disquieting is that the response of banks about their inability to offer a proper solution to the grievance in over 43% of the cases was "they are following RBI guidelines". I think it is necessary for the customer relations personnel are adequately trained to guide customers with greater clarity.

While the focus of the conference is on secure banking, it is not adequate to ensure that all banking transactions are duly authorized and customer interests protected. It is important for banks to realize that they have a vital role and responsibility to ensure that appropriate risk management measures are in place particularly to address issues relating to money laundering and terrorist funding. I recall that an year or so back, we found on enquiry that about 3-4 cards issued overseas were used extensively in the ATMs of one bank resulting in cash withdrawal of over Rs.2.00 crore in a short span of three months. Obviously, whoever used the card was not a tourist on a shopping spree ! When the matter was brought to the notice of the bank, they conceded that with reasonable risk mitigation measures, the transactions could have been identified and remedial action initiated. In this regard, we at RBI also noticed that a bank overseas was offering prepaid cards which could be delivered in India by courier. While we had no idea about the KYC aspects overseas, these cards could be used at any ATM in India to withdraw cash. The implications of such a system to our country are not hard to imagine. While RBI stepped in to halt the use of these cards in India, it is important for banks to be vigilant against similar events and alert the appropriate authorities if necessary.

Another area of concern that has emerged relates to fraudsters soliciting information by directing unsuspecting customers to a website purported to be that of an authentic institution, through a link in the email. This has also happened when mails were received by members of the public that a huge amount was received in their name and held with the Reserve Bank of India. They were provided with a link which masqueraded as RBI website and inviting them to provide their bank account details. While RBI has cautioned the public through advertisements in the media, banks also need to be watchful. But an important question that begs an answer here is that in many of these cases money has been paid by the unsuspecting public into bank accounts from where the funds have been withdrawn. How did these accounts get opened in the first place? Are banks lax in observing KYC requirements? Is monitoring getting increasingly lackadaisical once the machines have taken over the work hitherto done manually?

Another challenge faced by the Industry is handling of systems, data and processes by third party vendors, which is a necessity today, and the need to have effective control over the actions of these vendors/ service providers. This is in addition to the internal threats as often computer criminals are employees of the same organization. So, while still aware of outside threats, banks have a new threat, inside violations concerning data at rest. Today's employees are able to easily export sensitive files and information via email, FTP or by copying data to portable media. Banks have to control over where their sensitive information is, how it is used, and who obtains it. (e.g customer data being compromised at Citi Account Online, Hyundai Capital and Sony)

Banking Industry has been conscious of the challenges to Security and appreciable efforts are being made by all the stakeholders in the context, viz. Governments, Regulators, banks and technology providers. As you know, a working group was constituted by RBI under the Chairmanship of Shri. G. Gopalakrishna, ED, RBI on Information security, Electronic Banking, Technology Risk management and cyber frauds which provides detailed

suggestions in areas relating to IT Governance, Information security, IT operations, Information system audit, Cyber frauds, Business Continuity Planning, customer education and legal issues arising out of use of IT.

The Group has given recommendations that need to be based on the nature and scope of activities engaged by banks and the technology environment prevalent in the bank and the support rendered by technology to the business processes. The major recommendations pertain to IT Governance. IT Operations, Information security, IT outsourcing, IS audit, Cyber fraud, Business Continuity Plan, Customer education and legal issues.

The Group has recommended the policies that should be in place for the areas quoted above and also the best practices to be adopted by banks for achieving optimum benefit of technology in a secure and safe manner. While the implementation of the recommendations is being looked into by a Working Group constituted by the IBA, the banks may do well to make a self-assessment of their position vis-à-vis the recommendations and initiate appropriate measures

Having stated as above I must add that the real challenge in this environment goes beyond merely providing additional technology solutions and increasingly complex security layers, and translates into providing secured banking while balancing the same against customer convenience requirements, which puts the regulators and security implementers on the horns of a dilemma. I would enumerate a few of such dilemmas here.

- One time password / two factor authentication is one of the methods in securing transactions. However, the essential requirement of such OTP being sent to the registered mobile of the customer leads to several issues/ inconvenience due to factors like network availability, restriction to a particular phone number, non-availability of the service when customer travels abroad, timing out of online transactions due to slow speed of OTP transmission etc. It also has cost implications for the customer as he has to pay for charges at international data transmission tariffs.
- Multilayer security by way of log-in password, transaction password and some confidential data confirmation make on-line transactions secure in a better manner. But, there are issues like memorizing of multiple passwords, „slogans" , pictures, answers to questions etc. and some transaction of urgent nature getting struck due to these problems and even online access getting blocked some times. This, coupled with the time taken for access re-activation, password generation etc.; which is sometimes a lengthy/ time taking process, causes irritation and inconvenience to the customer.
- In mobile banking the challenge is to decide the transaction value limits up to which unencrypted data can be transmitted for payments/ funds transfer. If the limits are set too tight there can be cost and efficiency implications while making it too lax may invite the risk of information getting compromised.
- Surveillance cameras help in making ATM transactions more secure, but there are issues about privacy and more so, customer discomfort with the same.

Overall, while the challenges to security are stiff and increasing by the day, being alive to threats is more important. This involves resources - human and monetary, attitude and aptitude. Having reasonably secured card not present transactions, RBI has started looking at enhancing security of card present transactions. If we recognize that compromise of cards could happen, not only at ATMs but also at to over half-a-million and still growing PoS terminals, the task is indeed formidable. The questions that would arise are: Is a move to Chip based card system the only solution against the risk of skimming and cloning? Or is there a relatively less expensive alternative like a second factor authentication for all card present transactions? Should the 2FA be static or dynamic? How will it help if the static 2FA is compromised? Will a dynamic OTP really work without impacting the efficiency of the

merchant operations and inconvenience to the customers? As you may be aware, RBI constituted a Working Group to address these issues. The report of the Group which was placed on the public domain for comments on June 02, 2011 is now being processed. The Group has noted that Aadhar biometric data would serve as a secure second factor of authentication even for Magnetic Stripe Cards obviating the need mandating a switch over to EMV Chip and Pin card regime, which has cost implications for the industry. The Group has recommended that the need for a move to EMV Chip cards could be considered after 18 months depending on the progress of Aadhar. While the RBI is processing the report, we are aiming at a secure 2FA for all card present transactions without being prescriptive about the technology to be deployed for the purpose.

Innovative thinking and creative solutions by the industry, focused attention on enhancing customer awareness coupled with required investments in suitable technology for security risk mitigation will be imperative for ensuring optimal levels of banking security with appropriate customer convenience.

RBI is with you in your endeavor to offer secure and convenient online banking.

Thank you for your patience.