Fintech and Banks : Opportunities and Challenges[°]

Dr. Ramasastri, Director, Institute for Development and Research in Banking Technology (IDRBT), dignitaries for today's Awards function, ladies and gentlemen,

At the outset let me thank the IDRBT for inviting me to deliver the key note address at a function which felicitates best performing banks in the use of Information and Communications Technology, and as on a topic which is of particular relevance in the world of today**.**

We are all in the midst of a sea change, which has been brought about by technology. More than two centuries ago, the Industrial Revolution was the harbinger of a major change which resulted in the comforts of life which we enjoy today, with the manufacturing sector being the backbone of the economic revolution. There have been changes in agriculture methods, which have paved the way for new, improved farming methods and increased food grain production. The new millennium has seen the growth of services which have now become a significant economic contributor in many countries of the world and notably in the Indian context too. And, at the heart of the services sector is the financial sector with specific focus on the banking sector without which most businesses may find it difficult to even exist. And at the heart of the banking sector is the definitive role played by Information Technology or IT as commonly referred to.

[°] Keynote Address at the 13th Banking Technology Excellence Technology Awards, Institute for Development and Research in Banking Technology, Hyderabad, India, September 1, 2017

If one were to read Alvin Toffler's well-read book 'The Third Wave', it may be a startling revelation to note that many of the predictions made by him more than four decades ago are now real. Not merely real but frighteningly risky too. According to Toffler, since the late 1950s, most nations have been moving away from a Second Wave Society into what he refers to as a Third Wave Society, one based on actionable knowledge as a primary resource. His description of the present super-industrial society has brought in various concepts such as the Information Age, Space Age, Electronic Era, Global Village, technetronic age, scientific-technological revolution and so on, all of which are characterised by diversity and knowledge-based operations. Toffler had believed that the current era's greatest turning point is the creation of wealth in outer space. According to him, wealth is created everywhere (globalisation), nowhere (cyberspace), and out there (outer space).

IT systems are at the centre of all our operations in the world of today. The mobile phone that we have, the car which drops us to our office, the coffee vending machine and the microwave oven in the cafeteria, the personal digital assistant or the computer which we use in the bank where we have our money deposited and the credit or debit card which we use to pay for the goods bough from the departmental store – all have IT as an essential ingredient. Perhaps there is no industry in the world which has witnessed such rapid growth in the last two decades such as the IT industry and the banking sector has been one of the largest beneficiaries of this boom, with the use of computers in a large scale. We are all aware of the initial use of Ledger Posting Machines which soon gave way to the Advanced Ledger Posting Machines (a pseudonym for Computers) in the late eighties. From then on, the journey of IT in banks has been very

impressive and the metamorphosis has now given way to FIntech as it is commonly referred to. Is Fintech ushering in a new revolution? The answer is an affirmative 'Yes' and the disruptive role of Fintech is making financial services delivery by banks more easy to the user, more efficient to banks, more convenient to customers and more amenable to banks. There is even a perceived threat from Fintech companies – with soothsayers predicting that the future generation of banks are Fintech companies which undertake banking operations.

Before I dwell in detail about the role of Fintech in banks, let me pause for a while and look backwards on the journey of the Institute for Development and Research in Banking Technology (IDRBT). IDRBT was established by the Reserve Bank of India, in 1995, for research and development in Banking Technology at a time when use of Technology in Banking was in its infancy. The Institute commenced its tasks of training and educating officers of commercial banks, while at the same time concentrating on research activities relating to Banking Technology. It also managed the INdian FInancial NETwork (INFINET) for the use of banks, at a time when communications networks were still unheard of. True to the spirit of its name, the Institute has been focusing on areas relevant to banking technology for the past two decades. In line with the requirements of banks today, the areas of research undertaken by the Institute include Cyber Security, Analytics, Cloud Computing, Financial Inclusion and Payment Systems, with special emphasis on Mobile Payments.

Recognising the need for continuous upgradation of security which can be based on appropriate Research and Development, the RBI had mandated that IDRBT focuses on R&D in Information and Communication

security, mobile security and other Information Security related areas of work. Documents outlining the best practices in the respective Information Security areas have been published by this institute which have been incorporated in the IT based functioning of banks in the country. Some of the publications are : ‘Data Quality Framework’, ‘Cloud Security Framework’, Information Security Framework for the Indian Banking Industry’, Information Security Governance for the Indian Banking Sector, Holistic CRM and Analytics for the Indian Banking Industry’. Today’s release of more frameworks is another feather in IDRBT’s cap.

IDRBT instituted the Banking Technology Excellence Awards more than a decade ago and this year’s edition represents a very special number – 13. Although regarded as unlucky by many in the West, I am convinced that this year will herald glad tidings to banks as they prepare themselves to exploit the opportunities as also manage the challenges which are unfurled by Fintech.

While IT improves the quality of life and make tasks more efficient, IT also brings with it innumerable risks which at times could countermine the very benefits it offers. As we incorporate systems and practices to cover these threats, new fronts open up. Cyber security thus needs to be addressed adequately and continuously.

Why is it that cyber security assumes great significance for the banking sector? First, this sector has been an early adopter of IT and today no banks can even think of operations without IT. Second, IT has helped financial institutions to grow and provide better services to their customers. Third, new delivery channels are evolving all based on IT.

These delivery channels provide customer convenience; they are, however, vulnerable to cyber attacks. Fourth, cyber attacks on the banking sector implies that there is money to be gained by the attacker. Fifth, the financial sector is a prime target of cyber attacks both because of the data they carry and the impact that a disruption on their operations could have on the economy. And finally, security cordons cannot always be totally perfect. All these have made the IT intensive banking sector as a prime target for cyber attacks.

Having outlined all these, we need to ensure that there is no negative impact on the banks and that the customers have confidence in their operations so as to ensure that their money is safe and secure. The Reserve Bank, as the regulator of banks in India thus considers it of prime importance that banks ensure adequate safety and security of their IT systems. This is where Fintech can play a vital role.

The mere unauthorized access to IT systems of banks is now not a possibility since access to the main IT systems of banks are now highly complex and available only to authorized users. Cyber attackers have therefore, changed their strategies. While they exploit vulnerabilities in software and networks and these are being provided with due focus by every organization, a new weak link is now emerging – who is the customer.

How many of us have received unsolicited mails informing about a lottery or a huge sum of money which we are supposed to get? Maybe all of us here have got such messages. How many of us have received unsolicited messages seeking details such as the User Id, password, card details,

CVV and the like? Maybe most of us here have got such messages, and I am sure that most of us just ignored them. But then, sometimes when the messages appear authentic (or sound authentic if it is a voice based telephonic request) and some of us may tend to fall a prey to these. And that's the beginning of a cyber attack and the loss of money in no time! Let me juxtapose this with the good old brick and mortar personal banking: If there was a request from somebody claiming to be a representative of a bank and if he were to ask you for your signature, would any body here venture to share the same? The answer is a definite No. But then when it comes to IT based systems (such as cards, Internet and Mobile access to bank accounts), we are not that careful in not sharing confidential and sensitive information which are security features. This is probably because of inadequate awareness by the customer but more importantly this is on account if the mindset created in this world of the Internet where one does not seek but get sought after. We are all bombarded with hordes of information, inputs, advice, news, tips, questions, spicy previews….the list is endless as far as IT based systems are concerned. Data breach arising from phishing attacks and social engineering continues to be on the rise. Banks are making significant efforts to educate the user on safe banking but it is often found to be inadequate in the face of a targeted attack. Social media provides the platform required for an attacker to mine information on an individual. This information is then used to make the user believe that he is communicating with a legitimate source. With easier access to social media and the tendency to share personal information the numbers of users that are exposed to such attacks will continue to increase. Thus, it has become an accepted culture that we get unsolicited requests and responding to these is taken as a normal activity. This needs to be stopped, especially for IT based banking. Let us take an oath that we shall requisition the services which we need and we shall not

accept any service which comes unasked even if it is attractive. This mindset change may keep cyber attackers at bay – at least till they fathom out a new psychological weakness in mankind.

An important component of IT Security relates to Authentication. A user of an IT system is authenticated based on a set of predefined parameters. At the most elementary level, these could be in the form of User Identification (User ID) and password, but these could scale up to more effective systems using biometric authentication systems and other enhancements including digital signatures with local device end validation which would obviate the need for information travelling on a network. These systems are now part of the IT Security systems of banks which add on to robust Information Security; you would all have also experienced the second factor authentication for 'Card Not Present' transactions (now called as 3d Secure by Master Card and Verified by VISA), which is a simple yet safe mechanism which was pioneered by us in India and now adopted almost all over the world.

As new products and delivery channels using large scale IT and Communication systems gain ground, the need for enhanced security also gains importance. This is where Fintechs have mushroomed. They provide solutions to the complex needs of banks and their customers; they aim to provide products and services which are affordable and convenient to use.

You would all be familiar with the phrase "The Internet of things". This is fast catching up in the banking world as well. Most of us would love to use our smart phones for all types of functions including the conduct of

banking transactions. The smart phones available today are capable of carrying out a whole set of tasks which were hitherto unimaginable. Mobile devices, although becoming ubiquitous are also an attractive and easy target for cyber attackers. The question to be asked is not only whether the mobile device is secure but also whether it cannot be misused in case of loss or if it falls into unauthorized hands. Today, a typical Indian home has mobile phones, tablets, laptops, smart TVs and gaming devices all connected to the Internet and with each other. It is estimated that by 2020 there would be 30 billion wireless devices connected to the Internet of things. Each of these devices would be capable of communicating with each other on behalf of the user. Most of these peripheral systems have not been designed with focus on security but rather on ease of use and convenience. With a large number of unsecure devices connected on the same network, the more secure ones also become vulnerable. The tendency to exploit the weakness in a less secure but trusted device and then to use that device to attack critical and well protected resources will increase. This is where the Fintechs can play an important role – they can develop products and services which can overlay on these systems for either enhanced security or for providing additional capabilities.

In the world of today, two words are gaining importance – cyber security. If cyber security has to be effective, there needs to be a framework to combat cyber incidents. Current approaches in this regard are either inefficient or ineffective due to two reasons: firstly, the educational approaches usually take a long time to reach most of the public, and fraudsters are very clever and able to bring upon new scenarios to victimize people within a relatively short time. Secondly, fraudsters are usually well organized groups, which results in an asymmetric war

between individuals and the fraudsters. Therefore, techniques should be developed to empower individuals and prevent them from being victimized. For example, more advanced techniques, such as data mining for anomaly detection should be developed for online surveillance and detection for anomaly transactions. While IT based tools to combat cyber security incidents are relevant, use of data analytics to determine customer behavior may be also beneficial to aid in cyber security. Thus, customer behavior patterns could be mapped and if a deviation occurs, there could be an enhanced security trigger such as an SMS based approval for a specific IT based transaction. This may add a bit to customer inconvenience but it would certainly aid in reducing frauds thus conforming to the age old maxim : ‘Better to be safe than sorry’. Fintechs have the potential to provide systems and solutions which can take care of these requirements.

FIntechs are also playing a vital role in the emerging areas of Payment and Settlement Systems. We are all aware of the innovative systems which cropped up during the Demonetisation period. Most of these were developed, implemented and managed by Fintechs. Use of QR for payments is perhaps and easy, convenient and cost-effective way – this is a product of a Fintech. Can Fintechs exist in isolation? The answer to this is ‘No’. Collobration by banks and Fintechs will yield smart outcomes and smart banks will find smarter ways for better use of Fintechs to serve smarter customers who are now demanding better, easy-to-use services.

The marriage between FIntech and Banking also has its attendant challenges. Like any other vendor based operational structure, the risks of outsourcing do exist. An approach to minimize these risks is to perhaps

migrate to co-sourcing with specific role clarity. Similarly, we should we do not abdicate the core banking tasks by banks has to be taken care of. The need to have an understanding of the products and services offered by Fintechs, the relationships with the Banking Systems of banks and the control measures in place also have to be evaluated and suitable frameworks put in place to ensure that no additional risks emanate. Banks also need to understand the scope of collaboration. They have to ensure that the systems they get for use are robust and secure. And above all banks have to ensure the continuity of products and services from the Fintech companies.

Since I am now at IDRBT, let me dream a bit on a Fintech based banking facilitation. I shall take the example of Global Positioning Systems (GPS) which allows just-in-time (JIT) productivity thanks to precise tracking of the movements in every part of the chain comprising the manufacturing organisation. GPS is also becoming increasingly embedded in air traffic control, and satellites increase agricultural productivity as also better fishing outputs. In respect of banking, GPS holds exciting challenges for the future which could be a quantum jump from the fledgling initiatives currently being witnessed in the form of Internet and Mobile Banking. We are all aware of the key role played by satellites in synchronising precision time and data streams for maps and cellphone calls. Many of you may be avid users of Google maps to know precise directions to a particular destination, but how many of you would believe that GPS also has a role to play in the functioning of the Automated Teller Machine (ATM)? No, I am not hinting at the use of GPS for locating a nearby ATM, but I am referring to the way a bank could use GPS for monitoring use of the tracking a vehicle carrying currency notes for being refilled into ATMs and

even to track a customer who have used a particular ATM. They key common element at the base of all these new initiatives (Internet Banking, Mobile Banking and GPS based banking service facilitation) is the role played by Fintechs.

Let me now talk a bit on something different but a vital necessity. There has been a tendency to get good security products from Fintechs pertaining to and get pseudo comfort. It is not just the hardware and software that provide good security. Some of the breaches observed recently are not really technology breaches. They are breaches in control. That employees do not adhere to the well laid our processes and procedures is very dangerous. Putting in effective controls systems and ensuring employees follow them is the challenge to banks. Who ahs to be responsible for this – Fintechs or the banks?

There is also the need to exercise caution on the most critical part of cyber security. If I consider that security has four pillars – governance, policy, systems and awareness - I consider that the fourth is the most difficult to achieve. Awareness among all levels and segments of employees by itself is a challenge. A bigger challenge is to bring awareness among all its customers. The IDRBT's training and development oriented efforts address this requirement.

I have tried to outline some of the challenges which we are facing in the role of Fintechs in Banking. There are areas of comfort and there are areas of challenge; in today's world, one needs to ensure that there is co-operation and competition, juxtaposed in the form of 'comperation or 'co-opetition'. I am sure that I have been able to ignite the thought processes

in all of you to work towards a more symbiotic relaytionship between Fintechs and Banks to result in a safe and secure yet IT based banking world. We shall be able to achieve this; nay, we have to achieve this. Given the high level of adaptability of the Banking sector, I have n doubts the Indian Banks will soon be able to function as leaders which the rest of the world will follow.

The awards of today reflect the excellence achieved by all banks in the country. The best performers are being felicitated today; the others will certainly shore up and soon so as to get recognition soon. The awards reflect the high standards of IT in Banking; I am sure that today's award are the precursor for further enhanced, successful, safe and secure banking in the days to come. My compliments to the banks which are receiving their honours today and best wishes to the others who, I am sure, will finds their place in the years to follow.

I wish each and every one assembled here all success in the various initiatives undertaken; the future lies in innovation and I look forward to an era of innovative, FIntech coupled banking in the country.

Thank you.