S S Mundra: Fraud risk management in banks - the do's and don'ts

Keynote address by Mr S S Mundra, Deputy Governor of the Reserve Bank of India, at the Seminar on Financial Crimes Management, arranged by the Centre for Advanced Financial Research and Learning (CAFRAL), Mumbai, 30 January 2017.

* * *

Shri Gopalakrishna, Director, CAFRAL; fellow bankers and participants of the Program on Financial Crimes Management! At the outset, let me mention that this is the third occasion I am speaking on frauds in as many months. In November 2016, I spoke on “Fraud Risk Management in Banks – Major Concerns and 12 Sutras for Bankers” and last month I spoke on “Fraud Risk Management – Forging Partnership between Public and Private sector banks” in which I focused on the ‘contemporary scene’, ‘challenges’ and ‘what more we could do’ to strengthen the defences against frauds in collective manner. It cannot be sheer coincidence that I am speaking on this issue so frequently. It has probably to do with both- a sharp increase in number of frauds in the banking sector coinciding with a greater appreciation of fraud risk in the system. My involvement in these seminars/workshops also underlines the importance that RBI, as banking supervisor, attaches to the management of fraud risk in the system. Each time I speak on the issue I do so with a fervent hope that each participant in these seminars develops greater commitment and sensitivity to mitigating and managing fraud risk in his/her respective organisation. Today I intend to explore few other dimensions of the broad theme of fraud risk management. But before I begin, let me commend CAFRAL for organising this event and providing a platform for the senior officials of the banks to gather and brainstorm on this issue of critical importance.

In the first section of my speech today, I would focus on cyber security and cyber frauds while in the second section I will highlight a few concerns outside the cyberspace.

Cyber security & frauds

2. In recent times, we have seen several high profile cyber-incidents both in India as well as globally. You will remember the Bangladesh Bank incident which rattled banks/central banks and forced us to look more closely at cyber security risks. There is an increasing trend in incidents pertaining to theft of personal information, abuse of ATMs and Distributed Denial of Service (DDoS) attacks on various banks. We have already witnessed an attempt to defraud a bank by abusing the SWIFT messaging system which thankfully could be salvaged post event without any apparent monetary loss. We also continue to receive information on several other cyber incidents- be it ransomware attack, ATM / Debit card incident or unauthorised access to bank servers. Phishing / Vishing also continue to haunt bank customers with such attacks becoming more and more sophisticated.

3. Technology adoption by banks and other financial entities has increased manifold in the recent years and today if a bank is not present in the digital world it would be well-nigh impossible for it to compete in the market. As technology evolves from being an enabler and differentiator to being at the core of the banks’ operations, associated issues of security need to be addressed comprehensively.

4. Post withdrawal of legal tender character of ₹ 500 and ₹ 1000 bank notes, there has been a phenomenal push towards digital mode of payment across the country. Aadhaar Enabled Payment Systems are gaining currency and the recent launch of ‘BHIM’ app for facilitating payments is another welcome move. While increasing adoption of digital payment technology would bring in several benefits to the economy, we need to be conscious of security aspects as well. Given this backdrop, let us look at some of the developments internationally.

5. In October 2016, G-7 countries came out with what is called as ‘Fundamental Elements of

Cyber Security for the Financial Sector', which covers cybersecurity strategy and framework, governance, risk and control assessment, monitoring, response, recovery, information sharing and continuous learning as key elements. The Committee on Payments and Market Infrastructures (CPMI), BIS and the International Organization of Securities Commissions (IOSCO) have issued *Guidance on cyber resilience for financial market infrastructures (FMIs) which also* emphasises on the importance for authorities to cooperate to support broader financial stability objectives. The Bank of England (BoE) has implemented "CBEST", a new framework for testing cyber security vulnerabilities, particularly in respect of core financial sector entities. Hong Kong Monetary Authority has announced the launch of a "Cybersecurity Fortification Initiative" (CFI), a comprehensive initiative aiming to raise the level of cybersecurity of banks.

6. Closer home, RBI issued a circular on Cyber Security Framework in Banks on June 2, 2016 mandating cyber security preparedness. A specialised cell (C-SITE) has been created within the supervision department of RBI to conduct detailed IT examination of banks' cyber security preparedness, to identify the gaps and to monitor the progress of remedial measures. More than 30 major banks are slated to be covered under detailed IT examination during 2016-17 and all banks by 2017-18. RBI's IT subsidiary (the Reserve Bank Information Technology (ReBIT) Pvt Ltd has also become operational with a mandate to focus on issues around IT systems and cyber security (including related research) of the financial sector and to also assist in the audit and assessment of the entities regulated by the Reserve Bank.

7. In terms of June 2 circular, banks were advised to assess the gaps in their preparedness vis a vis the baseline requirements prescribed by RBI and to draw a time bound plan to bridge the gaps urgently. The assessment reveals that barring a few banks the gaps are indeed significant, more so in respect of public sector banks. This warrants immediate and continued attention of the Board and the senior management of the banks. In the changed world, if bank boards do not have expertise in this area, it would become a handicap in the smooth operations of banks. Second, the traditional ways of allocating budgets for IT services in general and cyber security in particular need to undergo a radical change leading to need based assessment and cost effective solutions. The scare that was created during the recent ATM/Debit card incident clearly indicates that cyber security requires top attention by the Board. A few days ago, Risk.Net published an article on the Top 10 Operational Risks for 2017 and indicated Cyber Risk as the top most risk in the minds of Chief Risk Officers.

8. Against this backdrop, the involvement of the Board / Senior Management in appointing Chief Information Security Officers is becoming increasingly crucial. ***It is important that CISO is sufficiently senior in hierarchy***; understands technology well; appreciates the security aspects of all the technologies adopted by the bank; is responsive and ***is sufficiently enabled to stall launch of unsecure products***, whenever necessary. However, ground realities do not provide the needed comfort. I want to use this forum to reiterate that the role of CISO needs to be clearly articulated and reinforced immediately.

9. Our June 2 circular also mandates having a separate cyber security policy and cyber crisis management plan in place. We have observed that in many cases, the banks react to cyber incidents in a knee jerk and an ad hoc manner which at times has a potential to jeopardise future investigations. Having a thorough plan of action with clearly identified roles and responsibilities in the event of cyber incidents is a must in today's environment.

10. The old adage, prevention is better than cure applies to cyber security as well. Banks need to have a robust defence mechanism against cyber incidents at all times. However, our observation is that many a times, certain finer details such as configuration of devices, patch management, OEM supported software, password management or port management, are ignored or entirely left to the vendors resulting in an undesirable impact. Statistics suggest that it takes on an average about 6 months to detect cyber-attacks by outsiders and longer in cases where attacks

are by insiders. Thus, early detection and response assumes significant importance. Banks need to build capabilities to detect cyber-attacks early and respond to them quickly. Recovery from the incident is another aspect that needs to be well thought out.

11. The world has learnt that in dealing with cyber-attacks, awareness and sharing of information plays an important role. Knowledge on cyber related aspects is relevant for all the stakeholders including the Board members. We often observe that this key premise is ignored.

12. RBI has mandated that all unusual cyber-incidents have to be reported within 2 to 6 hours invariably. We observe that banks take much longer time in reporting the incident. Once reported, the results of root cause analysis as well as findings of forensic audit also need to be shared promptly. You would appreciate that timely reporting of cyber incidents is very crucial to enable issuance of suitable cautionary advisories to other banks.

13. In a nutshell, all stakeholders must work collectively to guard and fight against the menace of cyber threat. To quote our Prime Minister, "I dream of a DIGITAL INDIA where: Cyber Security becomes an integral part of our National Security[1]" Yes, when such message comes from the highest authority in the country, we need no further stimulus for action. I am sure that this Program will leave you with many takeaways and enable you to be a change agent within your respective institutions for securing the IT infrastructure as well as for educating the customers on how to avoid becoming a victim of fraud.

14. Before I move beyond the cyberspace and talk about other frauds, let me mention three issues related to cyber security that I wish the participants to deliberate upon during the course of the Seminar and one issue for the policy makers to ponder over.

a. The rate at which technology is undergoing a change is overwhelming. Contrary to that, human beings are slow learners and slower to adapt to changes, especially if it is a new technology. Against this background, the question that we need to ask ourselves is whether there is a need to employ newer and newer technology enabled products at a fast pace or are we merely doing this since competition has done so? Are you convinced that the new product would significantly enhance the efficiencies & enable better customer experience? My point is frequent introduction of new technology may only end up stretching human resources beyond their capabilities and might eventually prove counter-productive.

b. One trend that has been increasingly witnessed in recent instances of cyber fraud is introduction of malware in the computer systems by the fraudsters that sit ideal for days and months together before striking. These malwares are also known to self –destruct after they have achieved their desired objective. This is a really scary situation and hence, we need to be not only on continuous guard to identify the vulnerabilities that exist in our systems and to plug them but also scout for innocuous looking unknown programmes/malware from time to time.

c. The next aspect that I wish to highlight is around human behaviour. We have always known banking to be a relationship built on trust. However, when we talk about cyber security I tend to believe that 'zero trust' is the way to address it. What I am hinting at is that physical and logical access controls must work as designed and only such employees who 'need to know' the intricacies of the application software/programmes must have access to them.

15. Finally, I want to raise the issue of cyber literacy for consideration of the policy makers. As we go whole hog into the digital world, it is imperative that the employees as well as customers are cyber literate. I understand that some countries like Israel, have introduced cyber awareness in their high school curriculum. Perhaps, we also need to think on similar lines. With moderate levels of general literacy in our country, this could be a tall order, but nevertheless it is a goal worth pursuing relentlessly.

Let me now move from the cyber space to an earthly level.

Advances related frauds

16. During the FY 2016, advances related frauds constituted nearly 92% of the total frauds reported by all banks. This was more pronounced in case of PSU banks and less in case of private and foreign banks. In almost all the cases, we observed that the exposure had got seasoned as an NPA for 3 to 4 years before the borrower was declared as fraudulent. As a consequence, the gap between the date of occurrence and detection has been widening. Further, the gap between first bank and the last bank reporting the borrowal account as fraud to RBI is also very long. What is the concern here? As you know 'fraud' is a criminal offence and any delay on the part of the bankers in initially red flagging an exposure and subsequently declaring it as a fraud will have far reaching implications on the employee conduct and internal governance standard. Banks and bankers could be charged for abetting the criminal offence. My call to you therefore, is to identify and declare the account as fraud without wasting time. The best course of action would be to follow the instructions in letter and spirit and take a responsible and pro-active stand while attending consortium meetings.

17. As a penal measure borrowers who have committed a fraud in the account are debarred from availing bank finance from banks/FIs/NBFCs etc., for a period of five years from the date of full payment of the defrauded amount. After this period, it is for individual institutions to take a call on whether to lend to such a borrower. Anecdotal evidence and our transaction testing on the ground has suggested that this instruction is not always being followed. Recently, we had come across a case where a bank had extended a 'hand holding operation' facility in case of very large fraud account.

18. Frauds in the area of cheque cloning continue to be one of the areas of concern for us. We have come across cases where though the original cheques remained in the custody of the customer, cheques with the same series were presented and encashed by fraudsters. RBI has issued guidelines in the issue to the banks in November 2014 and it is necessary that the instructions are followed to prevent fraudulent practices.

People risk

19. In most of the PSU banks the demographic profile of the employees is very unfavourable and massive recruitment is happening across the banks at the entry level. While banks are augmenting the HR stock, most of them do not have the capacity to train, build and absorb them. In the process the banks are adding significant people risk.

20. Another form in which people risk can manifest is on account of gap in understanding of technology between two sets of employees, colloquially called "digital immigrants" (older generation) and the "digital natives" (the newer generation). Especially in the public sector banks which suffer from a "Missing Middle", the knowledge gap between the supervisors and supervised in the area of digital can be very stark and might result in loose controls. It is, therefore, important for the Board and Top Management of banks to look for ways to mitigate the people risk as part of the overall Fraud Risk Management Framework.

Conclusion

21. I am of the view that only eternal vigilance can bring us closer to a fraud free eco-system. At the cost of repetition, I would like to reiterate the 12 important messages/sutras for bankers ***for Bankers that I had outlined in another seminar*** which according to me are key to a better fraud risk management. Like Sutras, which are short pithy instructive sayings, these messages are simple and straightforward.

Sutra 1: Have a ROBUST Fraud risk identification, event reporting, control, allocation and mitigation framework. 'Four eyes principle' must be followed in all sensitive areas without compromise.

Sutra 2: Follow the 5 ‘Cs” of CREDIT - Capacity, Capital, Collateral, Conditions and Character.

Sutra 3: Bring in a CULTURE of eternal vigilance, strong internal control and compliance. Please remember Fraud is criminal offence.

Sutra 4: Remember that the solution for TECHNOLOGICAL CHALLENGES is not always more technology.

Sutra 5: Institute checks and balances to calibrate PEOPLE RISK. High rate of attrition is a new normal which we have to face. Under the circumstances, it is important that the newly recruited staff is appropriately trained to work at the desk he/she is attached to. I feel it would also be useful for the newly recruited staff to have properly documented systems and rule books alongside some kind of a FAQ support.

Sutra 6: EMPOWER fraud risk managers adequately.

Sutra 7: Use extensively the 3 Cs – CFR (Central Fraud Registry), CRILC and CREDIT BUREAUS

Sutra 8: Rely on MARKET INTELLIGENCE.

Sutra 9: Develop BUSINESS ANALYTICS tools.

Sutra 10: CUT LOSSES and exit when the situation so demands.

Sutra 11: DO NOT THROW GOOD MONEY after bad money in fraud cases.

Sutra 12: Comply with RBI Regulations in letter and spirit.

22. To conclude, I would say that programs like these are very useful towards acquiring requisite skill sets as the participants also get to learn from practical experiences of fellow practitioners. I once again thank Shri Gopalakrishna for inviting me here this morning and wish the rest of the Seminar all success.

[1] pib.nic.in/newsite/PrintRelease.aspx?relid=148097