Research Paper

Volume : 2 | Issue : 8 | August 2013 • ISSN No 2277 - 8179

E-Banking system in India and Cyber Frauds

Commerce

KEYWORDS : E-Banking, legal issues, RBI and working group on E-Banking

Parameshwara Assistant Professor, Department of studies and Research in Commerce, Mangalore University, Mangalagangotri- 574199

ABSTRACT

Innovations in technology will bring changes in the functions of banking system. It would not only help them bring improvements in their internal functioning but also enable them to provide better customer service. Technology will break all boundaries and encourage cross border banking business. E-banking helps us in overcoming the drawbacks of manual system, as computers are capable of storing, analyzing, consolidating, searching and presenting the data as per the user requirements with lot of speed and accuracy. Banks would have to undertake extensive Business Process Re-Engineering. Along with the development of technology, fraudulent use of the technology also emerged. The RBI, Government and the banks must develop fraud controlling mechanisms for the development of Banking services and customer trust. This paper highlights the concept of E-Banking, benefits, limitations, legal issues, working group formed by RBI on E- banking and recommendations of the working group.

Introduction: Innovations in technology will bring changes in the functions of banking system. It would not only help them bring improvements in their internal functioning but also enable them to provide better customer service. Technology will break all boundaries and encourage cross border banking business. Banks would have to undertake extensive Business Process Re-Engineering and tackle issues like how best to deliver products and services to customers, designing an appropriate organizational model to fully capture the benefits of technology and business process changes brought about, How to exploit technology for deriving economies of scale and how to create cost efficiencies, and How to create a customer - centric operation model. Banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking. Fraudsters have also followed customers into this space. However, the response of most of the banks to frauds in these areas needs further improvement, thereby avoiding putting the entire onus on the customer. There is also a lack of clarity amongst banks on the reporting of these instances as frauds.

Reserve Bank of India (RBI) has recently constituted a working group on information security, electronic banking, technology risk management and cyber frauds. The working group submitted its report in the recent past upon which public inputs were invited. After analysing the public inputs, the final draft has been recently released and notified by the RBI.RBI has also directed that all banks would have to create a position of chief information officers (CIOs) as well as security at the board level at the earliest. This direction was provided through the information (IT Vision 2011-17) and the recent notification of the draft report. This document has suggested many technological as well as legal reforms for banking sector of India.

E-Banking:

E-banking is the term that signifies and encompasses the entire sphere of technology initiatives that have taken place in the banking industry. E-banking is a generic term making use of electronic channels through telephone, mobile phones, internet etc. for delivery of banking services and products. The concept and scope of e-banking is still in the transitional stage. It increases efficiency in the sphere of effective payment and accounting system thereby enhancing the pace of delivery of banking services considerably. It allows customers to access banking services electronically such as to pay bills, transfer funds, view accounts or to obtain any banking information and advice. E-banking also facilitates new relationships with customers, regulatory authorities, suppliers and banking partners with digital-age tools. For example, customers and bank relationships will become more personalized, resulting in new modes of transaction processing and service delivery. Now, banks are faced with a number of important issues, for example how to take full advantage of new technology, how e-banking change the ways customers relate with the service provider, etc. The banking industry has been considerably influenced by expansion of technology.

E-banking helps us in overcoming the drawbacks of manual system, as computers are capable of storing, analyzing, consolidating, searching and presenting the data as per the user requirements with lot of speed and accuracy. Number of benefits accrues with the development of e- banking.

Benefits to the Banks: E-banking services help in increasing profits, provides competitive advantage with boundary less network to the banks, banks carry on business less with paper money and more with plastic money; have online transfer of funds, thus economizing on the cost of storage of huge stocks of currency notes and coins and by connecting with ATM and PO terminals, risk of cash overdraw can be eliminated in case of ATM credit and debit cards.

Benefits to the customers: E-banking provides 24 hours service to the customers for cash Withdrawal from any branch, quick and steady access to information, online purchase of goods and services and payments can be made for various purposes, customer can view his account balance, can get a statement of his account, can apply for loans, check the progress of his investments, review interest rates and collect other important information, It ensures assured quick payment and settlement to the various transactions made by the traders; it provides a variety of services to the businessmen on par with the international standards with low transaction cost, Cost and risk problems involved in handling cash which are very high in business transactions are avoided, It leads to the growth of global and local clientele base with the development of e-Banking, Other benefits include improved image, improved customer service, eliminating paper work, reduced waiting costs and enhanced flexibility.

Limitations:

- Online transactions take a toll on the relationship with the banker which the traditional visit to the branch office used to foster. Personal relationship with the staff at the banks comes handy when requesting for faster loan approval or a special service which may not be available to the public. The manager has many discretionary powers such as waiving of penal interest or service fees which were often taken advantage of by better acquaintance with the staff. Additionally personal contact also meant that the banker would provide essential financial advice and insights which are beneficial to the customer.

- There are many complex transactions which cannot be sorted out unless there is a face to face discussion with the manager that is not possible through e- banking. Solving specific issues and complaints requires physical visit to the bank and cannot be achieved through the internet. Online communication is neither clear nor pin pointed to help resolve many complex service issues. Certain services such as the notarization and bank signa-

ture guarantee cannot be accomplished online.

• This is the biggest pitfall of the e -banking scheme which needs to be guarded against by the common customer. Despite the host of sophisticated encryption software is designed to protect your account there is always a scope of hacking by smart elements in the cyber world. Hacker attacks, phishing, malware and other unauthorized activity are not uncommon on the net. Identity theft is yet another area of grave concern for those who rely exclusively on internet banking. Most banks have made it mandatory to display scanned copies of cleared checks online to prevent identity theft. It is essential to check bank's security policies and protections while opening an account and commencing the usage of online banking facilities.

Legal Issues:

i. Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer.

ii. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk.

iii. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers 'accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks.

iv. In Internet banking scenario there is very little scope for the banks to act on stop payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.

v. The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks.

Shri. G .Gopalakrishna Committee Recommendations on Cyber Frauds (2011):

Banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking with the developments in information technology. Fraudsters have also followed customers into this space. However, the response of most of the banks to frauds in these areas needs further improvement, thereby avoiding putting the entire onus on the customer. There is also a lack of clarity amongst banks on the reporting of these instances as frauds. The following are the key recommendations of the group.

• Most retail cyber frauds and electronic banking frauds would be of values less than Rs.1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is recommended that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values.

• The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent fraud risk management group in the bank. The group should be adequately staffed and headed by a senior official of the bank, not below the rank of General Manager/DGM.

• Fraud review councils should be set up by the fraud risk management group with various business groups in the bank. The council should consist of the head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet at least every quarter to review fraud trends and preventive steps taken that are specific to that business function/group.

• Various fraud prevention practices need to be followed by banks. These include fraud vulnerability assessments(for business functions and also delivery channels), review of new products and processes, putting in place fraud loss limits, root cause analysis for actual fraud cases above Rs.10 lakhs, reviewing cases where a unique modus operandi is involved, ensuring adequate data/information security measures, following KYC and Know your employee/vendor procedures, ensuring adequate physical security, sharing of best practices of fraud prevention and creation of fraud awareness among staff and customers.

• No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process needs to be analyzed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.

• Banks have started sharing negative/fraudulent list of accounts through CIBIL Detect. Banks should also start sharing the details of employees who have defrauded them so that they do not get hired by other banks/financial institutions.

• Quick fraud detection capability would enable a bank to reduce losses and also serve as a deterrent to fraudsters. Various important requirements recommended in this regard include setting up a transaction monitoring group within the fraud risk management group, alert generation and redressal mechanisms, dedicated e-mail id and phone number for reporting suspected frauds, mystery shopping and reviews.

• Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitization for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.

• It is widely accepted that fraud investigation is a specialized function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies.

• Apart from the categories of fraud that need to be reported

as per RBI Master Circular on Frauds dated July 2, 2010, it is recommended that this should also include frauds in the electronic channels and the variants of plastic cards used by banks and their customers to conclude financial transactions.

- It has been noted that there is lack of uniformity regarding the amount of fraud to be reported to RBI. Some banks report the net loss as the fraud amount (i.e. fraud amount minus recovery), while others report the gross amount. Some do not report a fraud if the entire amount is recovered. In the case of credit card frauds, some banks follow the practice of reporting the frauds net of chargeback credit received while others report the amount of the original transactions. To overcome such inconsistency, a uniform rule of reporting amounts involved in frauds is being recommended.

- A special mention needs to be made of frauds done by collusive merchants who use skimmed/stolen cards at the point of sale (POS) terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. Many banks do not report such cases stating that the banks which have issued the cards are the ones impacted. However, in these cases, the merchants cause undue loss to the bank by siphoning off the credit provided. Hence such cases should be reported as frauds.

- It has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another bank's ATM, there is a lack of clarity on who should report such a fraud to RBI. It is the bank acquiring the transaction that should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money.

- Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums.

- A positive way to create employee awareness is to reward employees who have gone beyond the call of duty and prevented frauds. Details of employees receiving such awards may be published in the fraud newsletters.

- In the case of online frauds, since the jurisdiction is not clear, there is ambiguity on where the police complaint should be filed and customers/banks have to shuttle between different police units on the point of jurisdiction. Cybercrime cells are not present in every part of the country. The matter of having a separate cell working on bank frauds in each state police department, authorized to register complaints from banks and get the investigations done on the same, needs to be taken up with respective police departments.

- To enhance investigation skills of the staff in the fraud risk management group, a training institute for financial forensic investigation may be set up by banks under the aegis of IBA.

- The experience of controlling/preventing frauds in banks should be shared between banks on a regular basis. The standing forum provided by the Indian Banks' Association (IBA) can be used to share best practices and further strengthen internal controls in respective banks.

- At each state, a Financial Crime Review Committee needs to be set up on frauds along the lines of the Security Committee that has been set up by the RBI to review security issues in banks with law enforcement authorities. The Committee can oversee the creation of awareness by banks among law enforcement agencies on new fraud types, especially technology based frauds.

- There needs to multi-lateral arrangements amongst banks to deal with on-line banking frauds. The lack of such an arrangement amongst banks may force a customer to interact with different banks/ organizations when more than one bank is involved. IBA could assist in facilitating such a mechanism.

Conclusion: Financial liberalization and technology revolution have allowed the developments of new and more efficient delivery and processing channels as well as more innovative products and services in banking industry. Banking institutions are facing competition not only from each other but also from non-bank financial intermediaries as well as from alternative sources of financing. India, need for providing better and customized services to the customers. Along with the development of technology, fraudulent use of the technology also emerged. The RBI, Government and the banks must develop fraud controlling mechanisms for the development of Banking services and customer trust.

REFERENCE

1. Daniel, E. (1999), Provision of electronic banking in the UK and Republic of Ireland, International Journal of Bank Marketing, Vol.17 (2), pp. 72-82. | 2. Akinci, S., Aksoy, S. and Atılgan, E. (2004), Adoption of internet banking among sophisticated consumer segments in an advanced developing country, International Journal of Bank Marketing, Vol.22 (3), pp. 212-32. | 3. Grabner-Kräuter, S., & Faullant, R. (2008), Consumer acceptance of internet banking: the influence of internet trust, International Journal of bank marketing, Vol.26 (7), pp. 483-504. | 4. Eriksson, K., Kerem, K., & Nilsson, D. (2008), the adoption of commercial innovations in the former Central and Eastern European markets. The case of internet banking in Estonia", International Journal of Bank Marketing, Vol.26 (3), pp. 154-69. | 5. Minakshi bhosale and dr. k.m. Nalawade (2012) e-banking services: comparative analysis of nationalized banks, ABHINAV National monthly refereed journal of research in commerce & management volume no.1, issue no.11 pp 212-219 | 6. http://cjnewsind.blogspot.in/2011/05/rbi-working-group-on-information.html | 7. http://www.niiconsulting.com/innovation/RBI%20Guidelines_Summary.pdf | 8. http://www.rajdeepandjoyeeta.com/internet-banking.html | 9. http://timesofindia.indiatimes.com/topic/RBI-guidelines./news/ | 10. http://kalyan-city.blogspot.com/2011/02/e-banking-online-banking-advantages-of.html | 11. http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243#ch7 | 12. Report of the Working Group on Electronic Banking, RBI 2011 |