RESEARCH PAPER | Economics | Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

Incorporation of Information Technology Act in Banking Transactions

KEYWORDS: Security,Information Technology, Banking

Dr. Ashok Shankarrao Pawar
Director, Vasantrao Naik Research Centre & Associate Professor, Department of Economics, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad (Maharashtra)

Dr. Sunita J. Rathod (Pawar)
Senior Lecturer, Maharashtra Education Service Group-A District Institute for Education and Training Divisional DIET, Nashik

Dr. Manish Parshuram Pawar
Department of P.G. Studies in Law, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad (Maharashtra)

Niraj J. Rathod
B. Tech Instrumentation and Control, College of Engieering Pune (COEP), System Engineer, EEEC Pune

ABSTRACT *The banking sector in India underwent an unprecedented transformation in the 1990s with the emergence of a large number of private as well as foreign multinational banks. As a result of the economic reforms, the number of banks increased rapidly. With the emergence of a large number of banks in the Indian economic set up, banking activities increased manifold and affected a large number of areas of operation of banks, particularly in the field of bank lending. Banks used to and still operate on the pattern of extending credit on the basis of security given by its customers associated with the bank. The facility of extending credit is recognition of the changing times in which banks have to operate in a changing and ever evolving economic scenario. Growing needs coupled with the realization of higher rate of investments is a compulsion giving birth to bank credit.*

The Indian Information Technology Act, 2000, basically a framework law, makes hacking a punishable offence under Section 66. Breach of information security is implicitly recognized as a penal offence in the form hacking. The appropriate government (central/state) is empowered to declare any computerized, account computer systematic or a computer network as a protected system. A ten year prison term and a hefty fine await any person who secures access to the secured computer systematic in contravention of the provisions of the law. Despite the deterrence characterized by the penal provisions of the IT Act, 2000, a lacuna in the law is that organizations and entities can take action against those who breach data security procedure, but they are not obliged to implement data security measures to protect consumers and clients. The IT Act does not lay down any such duty upon banks. Contrastingly, in UK, failure to undertake identification of new customers properly can create an array of risks for the bank. Under the Data Protection Act, 1998 an earring bank may face an action for damages if it fails to maintain adequate security precautions in respect of the data. Essentially, a legal duty is thrust upon the banks, to use reasonable care and skill in disseminating information to persons who access the banking networks either on the internet or though an ATM card.

Introduction
In India, a Bank liability would arise out of contract as there is no statute to the point. When liability is contractual it means that the bank is, by virtue of the contract, under an obligation to keep customers data secret. If transactions are being done on an open network such as the internet then in case of a security breach, an internet service provider (ISP) may be liable, in addition to the bank. Though ambiguity persists as regards liability of an internet service provider due to dearth of decided case law on the point.

Effective Currency Management
The impact of technology on the issuances of Bank Notes and Currency Management by Central bank is apparent. The technology offers us immense opportunities to significantly improve our performance of this core function. Given the high value and volume of currency in circulation, the vast geographic spread of currency operations, the largest distribution channel for the supply of currency, prevalent marked preference for cash and currency handling practices, currency management in India is a challenging and strenuous task. In 1999, the Reserve Bank of India announced a "Clean Note Policy" to bring about improvements of the quality of notes in circulation and technology has played an indispensable role in enabling the Bank to provide better quality notes to the general public. The information technology makes the task of currency management easy, effective, economical and speedier.

Monetary and Financial Stability
One of the critical activities undertaken by Central bank to ensure monetary and financial stability is to provide the banking sector with finality of settlement. The payment and settlement systems are the conduits through which monetary policy measures are transmitted to the financial and then the real economy. The information technology revolution has given rise to an extraordinary increase in financial activity across the globe. The progress of technology and the development of worldwide networks have significantly reduced the cost of global funds transfer. The technology has, in fact, placed at the disposal of Central bank a desirable selection of instruments to manage and eliminate risks in payment and settlement systems. Electronic trading platforms have reduced the gap between trade finalization and trade reporting and settlement and in the process have significantly reduced risks arising from the trading and settlement process. The Real Time Gross Settlement Systems (RTGS Systems) have been the preferred mode of settlement for large value funds transfers by central banks globally to minimize settlement and systemic risk. The RTGS systems would not have been possible without the network and information system capabilities to transmit payment messages to the settlement agency and process funds transfer instructions in real time. Delivery versus payment systems to reduce credit risks is securities

Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

settlement systems also owe their origin to the technological capability to harmonize positions in settlement banks and depositories in real time. The triumph of Information Technology has perhaps been the introduction of Continuous Linked Settlement, which ensures payment versus payment settlement of very large value foreign exchange transactions thus completely eliminating the risks in cross border transactions.

Challenges before Internet banking

The information technology in itself is not a panacea and it has to be effectively utilized. The concept of Internet banking cannot work unless and until we have a centralized body or institution, which can formulate guidelines, regulate, and monitor effectively the functioning of Internet banking. The most important requirement for the successful working of Internet banking is the adoption of the best security methods. This presupposes the existence of a uniform and the best available technological devices and methods to protect electronic banking transactions. In order for computerization to take care of the emerging needs, the recommendations of the Committee on Technology Up gradation in the Banking Sector (1999) may be considered. These are:

1. Need for standardization of hardware, operating systems, system software, and application software to facilitate interconnectivity of systems across branches
2. Need for high levels of security
3. Communication and networking – use of networks which would facilitate centralized databases and distributed processing
4. Need for a technology plan with periodical up gradation
5. Need for business process re-engineering
6. Need to address the issue of human relations in a computerized environment
7. Need for sharing of technology experiences
8. Need of Payment systems which use information technology tools. The Reserve Bank of India has played a lead role in this sphere of activity - with the introduction of cheque clearing using the MICR (Magnetic Ink Character Recognition) technology in the late eighties.

The Reserve Bank of India constituted a "Working Group on Internet Banking" which focused on three major areas of I-banking, i.e., (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues. These areas are selected in such a manner that the problems faced by banks and their customers can be minimized to the maximum possible extent. The Group recommended certain guidelines for the smooth and proper working of Internet banking. These centralized guidelines would bring uniformity in the selection and adoption of security measures, with special emphasis on a uniform procedure. The security of Internet banking transactions would not be jeopardized if these security mechanisms are adopted. This is because the success of Internet banking ultimately depends upon a uniform, secure and safe technological base, with the most advanced features. The RBI has accepted the recommendations of the Group, to be implemented in a phased manner.

Technology and Security Standards:

The technology and security standards are of prime importance as the entire base of Internet banking rests on it. If the technology and security standards are inadequate, then Internet banking will not provide the desired results and will collapse ultimately.

The RBI realizing this crucial requirement issued the following guidelines in this regard:

1. Banks should designate a network and database administrator with clearly defined roles.
2. Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology
3. Division, which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems.
4. Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.
5. At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank's system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a tasteful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert.
6. All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server.
7. PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. However, as it is not yet commonly available, banks should use the following alternative system during the transition, until the PKI is put in place:
8. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the banks themselves using a Certificate Server.
9. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself.
10. It is also recommended that all unnecessary services on the application server such as FTP (File Transfer Protocol), telnet should be disabled. The application server should be isolated from the e-mail server.
11. All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be reported and follow up action taken should be kept in mind while framing future policy. Banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis.
12. Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats.
13. . Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy. Business continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically.
14. All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form.
15. Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions, which give better security and control.

Internet banking and the Information Technology Act, 2000

The Internet banking cannot operate properly unless it is in conformity with the *Information Technology Act, 2000*. A holistic approach should be adopted, the purpose of which

Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

should be to bring uniformity and harmony between the provisions of the Act on the one hand and the guidelines issued by the RBI on the other. It must be appreciated that in case of conflict between the provisions of the following provisions of the Act have a direct bearing on the functioning of Internet Banking in India.

The authentication of electronic records for the purposes of Internet banking should be in accordance with the provisions of the Act. The electronic records duly maintained for the purposes of Internet banking would be recognized as legally valid and admissible. The digital signature affixed in a proper manner would satisfy the requirement of signing of a document for the purposes of Internet banking. Any kind of paper work, which is required to be filed in the government offices or its agencies, would be deemed to be duly filed if it is filed in the prescribed electronic form. Thus the paper formalities can be effectively substituted with electronic filings for Internet banking purposes.

The banking business requires certain documents or records to be retained for a fixed period. In Internet banking such documents or records can be retained in an electronic form. The rules, regulations, order, bye-law, notification or any other matter pertaining to Internet banking can be published in the Official Gazette or Electronic Gazette, as the case may be. The Internet banking presupposes the existence of attribution and certainty. If any electronic record is sent by the originator himself, by his agent, or by an information system programmed by or on behalf of the originator to operate automatically, then the electronic shall be attributed to the originator The requirement of acknowledgement of documents sent for the purposes of Internet banking is adequately safeguarded by the Act The Internet banking may require to determine the time and place of dispatch and receipt of electronic records. This problem can be easily solved by applying the provisions of the Act. The Internet banking would require the secured electronic records for its proper working. Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. A digital signature meeting the specified requirements would be deemed to be a secured digital signature for carrying out Internet banking transactions. The Central Government has the power to prescribe the security procedures to give effect to the provisions of the Act, having regard to the commercial circumstances prevailing at the time when the procedure was used. Thus, the Central Government can specify safety measures and security procedures for Internet banking under the provisions of the Act. The Controller of Certifying Authorities can issue licenses to the Certification Authority under the IT Act, 2000. The Certifying Authority is assisted by the Registration Authority, which is created at the level of the organizations subscribing to the services of the Certifying Authority .The Reserve Bank would function as a Registration Authority (RA) for the proper functioning of Internet banking.

Thus, the Information Technology Act, 2000 has laid down the basic legal framework conducive to the Internet banking in India. In case of any doubt or legal problem, the provisions of the Act can be safely relied upon. It must be noted that the object of the Act is to facilitate e-commerce and e-governance which are essential for the functioning of Internet banking in India. There may be challenges of Internet banking which cannot be tackled appropriately with the existing legal framework. To meet such challenge appropriate amendments can be made either to the Act itself or a separate new law dealing specifically with the Internet banking can be enacted.

With this it can be concluded that though banking customers have accessed towards the electronic payment systems still the risk involved in this could not be ignored. Hence to remove this defect we need a strong and separate legislation with the speedy and active enforcement machinery.

REFERENCE • Farooq Ahmed, Cyber Law and Banking 2004, First Edn. | • Amit Bajaj, Punit Bajaj: Law of Negotiable Instrument, 2006. | • Sharma Vakul, Information Technology Law & Practice, Second Edition 2007 | • Anil G. Rao, E-commerce Theory & Practice, Shree Niwas Publication. | • Ranbir Singh, Cyber Space & The Law Issue & Challenges, Nalsar University. | • Achary N. K., Commentary On The Right To Information Act, 2005, Asia Law House, 2008 | • Singh Jagwant, India Banking Industry Growth and Trends In Productivity, Deep and Deep Publication New Delhi, 2008 | • Kapoor Nidhi, Computerised Banking System In India, Sublime Publication.