Law Journals

Journal of Banking and Insurance Law

Volume 2, Issue 1
www.stmjournals.com

Contemporary Legal Issues in Indian E-Banking System

***Gunjan Bhagtani*[1, *]*, Janvi Pandya*[2]**
[1,2]Scholar, Faculty of Law, Maharaja Sayajirao University of Baroda, Vadodara, Gujarat, India.

Abstract

E-banking provides traditional banking services through the internet to the customers. The transition from physical banking to electronic banking in India has been a long and difficult approach. Numerous advantages have arisen to the banking sector and customers both with the introduction of e-banking. These include ease of doing banking to the customers and cost reduction and market share to the banks. However, with these advantages there comes a great risk of privacy and security to the stakeholders. There lies the imminent thereto of hacking and loss of valuable information and data. These concerns hamper the smooth functioning of the e-banking system. There has been a concern that Internet banking transactions may become a conduit for money laundering. The regulatory body of the Indian banking system is the Reserve Bank of India. It has stated atop on providing rules and regulations to tackle the issues arising from e-banking. There are many laws such as information technology act and consumer protection that take within their ambit banking services. From to time to time many notifications, circulars, and regulations have been issues by RBI with reference to e-banking and the issues underlying thereto. This paper is primarily theoretical in nature, aiming to critically analyse the prevalent laws for the electronic banking services and vis-a-vis international norms. The paper puts into perspective the prevalent legal issues arising out of e-banking.

Keywords. *Banking; Contemporary Issues; Reserve Bank of India; Banking Challenges; Issues; Legal Framework; Challenges*

Author for Correspondence E-mail: gunjanbhagtani564@gmail.com

INTRODUCTION

Banking is the growth engine of an economy. It provides numerous facilities to the enterprises, government and the common man therefore one cannot undermine the importance of a sound banking system. During the past few decades there has been a technology outburst in all sectors and banking has been one of the sectors to adopt information technology. Internet or e-banking means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking functions. E-banking has been defined in law lexicon as banking activities accessed by using a computer, employing modems and telephones. [1] In e-banking, 'e' stands for electronic and the banking has been defined as 'an acceptance of money from the public, for purpose of lending or investment of money, which is withdraw able by cheque, draft or otherwise' [2]. In layman terms it offers traditional banking services through the virtual medium. From the perspective of banking products and services being offered through Internet, Internet banking is nothing more than traditional banking services delivered through an electronic communication backbone, viz, Internet. But, in the process it has thrown open issues which have ramifications beyond what a new delivery channel would normally envisage and, hence, has compelled regulators world over to take note of this emerging channel. [3]

Some of the saline features of e-banking are:

1. It removes the traditional geographical barriers as it could reach out to customers of different countries / legal jurisdiction. This has raised the question of jurisdiction of law / supervisory system to which such transactions should be subjected,
2. It has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges,

3. It poses a strategic risk of loss of business to those banks who do not respond in time, to this new technology, being the efficient and cost-effective delivery mechanism of banking services,
4. It is cost effective and time saving to both banker and customer.
5. It facilitates transactions at all times including non-banking hours and holidays.

ISSUES IN E-BANKING:

Though e-banking has introduced ease of doing banking it has with it given rise to many issues and risks such as operational risks, security risks and privacy customer satisfaction and tax. Some of these issues are more sensitive than others for example privacy and security are the pivotal features around which e-banking has evolved.

(A) **Security and Privacy Risks:**

A recent study conducted 150 by PwC (2012) found that data security concerns and lack of clarity on regulatory stance are two major roadblocks in the adoption of internet banking (Cloud Computing) in Indian banks. Therefore, it is evident that with electronic banking on the rise, customers are vulnerable to the risks of e-banking frauds, even as regulations are becoming more stringent as far as know your customer (KYC) rules are concerned In this background, it is apparent that concern for security and privacy is the major roadblock in the adoption of e-banking services.

Security is a prominent risk factor in the system of e-banking, the easy access to financial accounts makes internet banking an easy target for hackers and online criminals. Security threats – measures approach includes several types of threats and measures – internal, external, human, non-human, accidental and intentional categories. [4] One of the primary methods of hacking or gaining access to confidential information is phishing [1]. Hackers operating via the internet could access, retrieve and use confidential customer information and also can implant virus. This may result in loss of data, theft of or tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service, cost of repairing these etc. The risk of lack of securitised transaction is faced by both customers and bankers, on the customers side the risk of data and identity theft and valuable information while on the banker's side they are more prone to money laundering and fraud.

Privacy is very important to mankind. However, while transacting online there is a risk of privacy as the customers have to disclose personal information, that if accessed by unauthorised persons would impact the individual. There have been many cases of identity theft and instances where valuable confidential data has been leaked.

(B**) Legal issues:**

Despite there being various international and national laws regarding e-banking there is still a lacuna in the smooth functioning of e-banking. Specifically, in terms of jurisdiction where international transactions take place. From the legal perspective the privacy procedure laid down by banks for providing access to internet banking needs to be recognized by law.

(C) **Operational issues and risks:**

Basel Committee on Banking Supervision, in its "Consultative Document on Operational Risk", defines "operational risk" as the risk of direct, or indirect, loss resulting from inadequate or failed internal processes, people and systems, or from external events. [5] Operational risk, also known as transactional risk, is the most common form of risk associated with e-banking. It takes the form of inaccurate processing of transactions, non-enforceability of contracts, compromises in data integrity, data privacy and confidentiality, unauthorized access / intrusion to bank's systems and transactions etc. [6] These risks can arise from weaknesses in design, implementation and monitoring of banks' information system. Besides inadequacies in technology, human factors like negligence by customers and employees, fraudulent activity of employees and crackers / hackers etc. can become potential source of operational risk. Often there is thin line of difference between operational risk and security risk and both terminologies are used interchangeably.

(D) **Authentication Issues**

One of the major challenges faced by banks involved in Internet banking is the issue regarding to authentication and the concerns arising in solving problems unique to electronic authentication such as issues of data integrity, non-repudiation, evidentiary standards, privacy, confidentiality issues and the consumer protection. The present legal regime does not set out the parameters as to the extent to which a person can be bound in respect of an electronic instruction purported to have been issued by him. Typically, the authentication process involves a security procedure. Methods and devices like the personal identification numbers (PIN), code numbers, telephone-PIN numbers, relationship numbers, passwords, account numbers and encryption are evolved to establish authenticity of an instruction. From a legal point of view, the security procedure requires to be recognized by law as a substitute for signature. Different countries have addressed these issues through specific laws dealing with digital signatures. In India, the Information Technology Act, 2000 in Section 3 (2) provides that any subscriber may authenticate an electronic record by affixing his digital signature. However, the Act only recognizes one particular technology as a means of authenticating the electronic records (viz, the asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record).

This might lead to the doubt of whether the law would recognize the existing methods used by the banks as a valid method of authenticating the transactions. The approach in the other countries has been to keep the legislation technology neutral.

LEGAL FRAMEWORK OF E-BANKING.

E Banking is not a separate business it is Banking using E Channels. Banking is regulated by RBI under RBI Act Subject to licensing Law regarding Electronic documents is contained in Information Technology Act 2000 As amended by Information technology Act 2008. There are various provisions of law, which are applicable to traditional banking activities and, are also applicable to e-banking. However, this does not overcome many problems, hence there is need for introducing more stringent rules and regulations specifically to meet the problems of e-banking. The legal framework of Indian banking system is governed by a set of enactments, i.e., The Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934 and Foreign Exchange Management Act, 1999, evidence act, contract act and so on. The Information Technology Act 2000 has attempted to address a number of e-commerce regulatory issues. Yet there exists a grey area, which has neither been spelt out properly nor has there been any workable modes of implementation suggested by Constitutional institutions.

ICICI Bank kicked off online banking in 1996, followed by a host of other banks. But even for the Internet as a whole, 1996 to 1998 marked the adoption phase, while usage increased only in 1999, owing to lower ISP online charges, increased PC penetration and a tech-friendly atmosphere.

However, the Public Sector Banks (PSUs) lagged behind in the race for adopting Internet banking practices. Amongst the PSUs, the State Bank of India took the lead.

(A) **Provisions of Information Technology Act, 2000**

After Information Technology Act 2000 notification on 17thOctober 2000 RBI constituted the S R Mittal Working group to recommend on regulation for Internet Banking Culminated in "Internet Banking Guidelines 2001" through an RBI circular dated June 14, 2001. [7] It mandates that those who wish to offer e-banking services must be licensed for the same. The guidelines primarily deal with: -

(a) Technology and security standards
(b) Legal issues
(c) Regulatory and supervisory issues.

In 2005 another circular was issued by RBI with reference to aforesaid guidelines. The position has since been reviewed and banks are advised that while the offering of Internet Banking services will continue to be governed

by the provisions of the above circular, no prior approval of the Reserve Bank of India will be required for offering Internet Banking services. [8] The other guidelines that were enumerated in the aforesaid circular are as follows:

a. The Internet banking policy has been approved by the Bank's Board.
b. The policy fits into the banks overall Information Technology and Information Security policy and ensures confidentiality of records and security systems.
c. The policy takes into account operational risk.
d. The policy clearly lays down the procedure to be followed in respect of 'Know Your Customer' requirements, and
e. The policy broadly meets the parameters laid down in our above circular.

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. This has raised the doubt whether the law would recognize the existing methods used by banks as valid methods of authentication. Further, Section 4 of ITA 2000Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is(a) rendered or made available in an electronic form; and(b) accessible so as to be usable for a subsequent reference. Also, under Section 72, the act provides for penalty for breach of privacy and confidentiality and section 79 of the Act has also provided for exclusion of liability of a network service provider for data travelling through their network subject to certain conditions. Later on, in 2008 substantial amendments were introduced in the Information Technology act, 2000. In January 2011, G Gopalakrishna Working group (GGWG) on E-Banking Security released its report notified with some changes on April 29, 2011 constitutes the current regulatory guidelines as an extension of IBG 2001. Additionally, Damodaran Committee (August 2011) on Customer Services and Banking Ombudsman conference (September 2011) has given further operational guidance for E Banking regulations. [9]

(B) **Provisions under Negotiable Instruments Act, 1881**

Other than this the Negotiable Instruments Amendment Act 2002 was notified and introduced the concept of Truncated Cheques and Cheques in E Form. [10] The act sought to amend various sections to incorporate provisions of e-banking. For example, Substitution of new section for section 6" Cheque".- A" cheque" is a bill of exchange drawn on a specified banker and not expressed to be payable otherwise than on demand and it includes the electronic image of a truncated cheque and a cheque in the electronic form. Explanation I- For the purposes of this section, the expressions-

(a) "a cheque in the electronic form" means a cheque which contains the exact mirror image of a paper cheque, and is generated, written and signed in a secure system ensuring the minimum safety standards with the use of digital signature (with or without biometrics signature) and asymmetric crypto system;
(b) "a truncated cheque" means a cheque which is truncated during the course of a clearing cycle, either by the clearing house or by the bank whether paying or receiving payment, immediately on generation of an electronic image for transmission, substituting the further physical movement of the cheque in writing. Explanation II.- For the purposes of this section, the expression" clearing house" means the clearing house managed by the Reserve Bank of India or a clearing house recognised as such by the Reserve Bank of India.'

(C) **Provisions under Income tax, Act, 1961**

Mode of Payment under the Income Tax Act, 1961: Section 40A (3) of the Income tax Act, 1961, dealing with deductible expenses, provides that in cases where the amount exceeds Rs. 20,000/-, the benefit of the said section will be available only if the payment is

made by a crossed cheque or a crossed bank draft. One of the services provided by the banks offering Internet banking service is the online transfer of funds between accounts where cheques are not used, in which the above benefit will not be available to the customers. [2] The primary intention behind the enactment of Section 40 A of the Income tax Act, 1961 is to check tax evasion by requiring payment to designated accounts. In the case of a funds transfer, the transfer of funds takes place only between identified accounts, which serves the same purpose as a crossed cheque or a crossed bank draft.

(D) **Indian Penal Code, 1860:**
Section 172 relating to documents to be produced before a Court of Justice includes electronic records, section 192 on 116 For example, section 29A, under which the word 'electronic record' was given meaning as, as in IT Act. 221 makes false entry in books of records,117 and section 463, the amendment is inserting false electronic record with the intent to cause damage or injury. The significant amendment was to section 464 of the Act which is as follows-'A person is said to make a false document or false electronic record, if, first, who dishonestly or fraudulently makes, signs, seals or executes a document or part of a document, or makes or transmits any electronic record or part any electronic record, or affixes any digital signature on any electronic record, or makes any mark denoting the execution of a document or the authenticity of the digital signature,118 with the intention of causing it to be believed that such document or part of a document was made, signed, sealed or executed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed or executed, or at a time at which he knows that it was not made, signed, sealed or executed; or affixed with, or

Secondly.- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made or executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration;

Thirdly.- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practiced upon him, he does not know the contents of the document or electronic record or the nature of the alteration. Then section 469, for the words "intending that the document forged" the words "intending that the document or electronic record forged" was substituted. Section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following words were substituted, "Whoever has in this possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code.

RBI has classified frauds on the basis of the provisions of the IPC. Misappropriation (Section 403 IPC) and criminal breach of trust (Section 405 IPC); b. Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property (Sections 477A, 378 and 120 A); c. Unauthorized credit facilities extended for reward or for illegal gratification; d. Negligence and cash shortages; e. Cheating (Section 415 IPC) and forgery (Section 463 IPC); f. Forgery of electronic records (Section 465 IPC); g. Bogus websites, cyber frauds, phishing (Section 420 of IPC) h. Irregularities in foreign exchange transactions.

(E**) Miscellaneous Provisions:**
Section 11 of the proposed Prevention of Money Laundering Bill, 1999 imposes an obligation on every Banking Company, Financial Institution and intermediary to maintain a record of all the transactions or

series of transactions taking place within a month, the nature and value of which may be prescribed by the Central Government. These records are to be maintained for a period of five years from the date of cessation of the transaction between the client and the banking company or the financial institution or the intermediary. This would apply to banks offering physical or Internet banking services. This will adequately guard against any misuse of the Internet banking services for the purpose of money laundering. Further the requirement of the banking companies to preserve specified ledgers, registers and other records for a period of 5 to 8 years, as per the Banking Companies. [3]

Section 4 of the Bankers' Books Evidence Act, 1891, provides that a certified copy of any entry in a banker's book shall in all legal proceedings be received as a prima facie evidence of the existence of such an entry. The Banking Companies (Period of Preservation of Records) Rules, 1985 promulgated by the Central Government requires banking companies to maintain ledgers, records, books and other documents for a period of 5 to 8 years.

The Consumer Protection Act 1986 defines the rights of consumers in India and is applicable to banking services as well. The issues of privacy, secrecy of consumers' accounts and the rights and liabilities of customers and banks, etc. in the context of Internet banking have been discussed in earlier paragraphs. In cases where bilateral agreements defining customer's rights and liabilities are adverse to consumers than what are enjoyed by them in the traditional banking scenario, it is debatable whether such agreements are legally tenable.

GUIDELINES ISSUED BY RESERVE BANK OF INDIA

Reserve Bank of India had set up a 'Working Group on Internet Banking' to examine different aspects of Internet Banking (I-banking). The Group had focused on three major areas of I-banking, i.e., (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues. A copy of the group's report is enclosed. RBI has accepted the recommendations of the Group to be implemented in a phased manner. The working group has recommended the following:

1. Banks should designate a network and database administrator with clearly defined roles as indicated in the Group's report. Banks should have a security policy duly approved by the Board of Directors.
2. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems.
3. 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.
4. 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.
5. For sensitive systems, an 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. PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services.
7. 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.

8. 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.
9. The information security officer and the information system auditor should undertake periodic penetration tests of the system.
10. 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.
11. 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.
12. 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.
13. 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. [11]

CONCLUSION AND SUGGESTIONS

Internet banking is the driving force of non-cash transactions to facilitate a seamless cash free economy. There is no doubt that if a nation wants its commerce and economy to flourish it must secure a safe and secure system of internet banking.

India as a nation has strived to do that and though the performance is a satisfying one it lacks behind when compared to the developed nation. The Indian e-banking market has emerged as a competitive and driven yet, there exist many loopholes in the regulatory framework. There are many threats and challenges that are arising.

As we bank across borders and barriers, the risk of privacy and security is the utmost challenge that worries both the banker and the customer. With the far-reaching technology system, it has difficult to fix liability on a specific person or individual. The legal provisions are abundant with regard to e-banking however with the dynamic upgrades in technology and means of banking new issues arise daily.

The author would like to suggest the following measures to combat the contemporary issues of e-banking:

1. The duty imposed on banks to maintain secrecy and confidentiality should be recognised statutorily. It should further be enforced by deterrent penal provisions. Also, the apex body, that is, RBI should conduct security audits.
2. The internal auditor or statutory auditor should ensure safety against misappropriation and fraud even at the micro level. The online audit trails must be preserved.
3. Automatic Teller Machines are also a medium of e-banking however they lack protection, the banks should introduce security measures like thumbprint, to gain greater security as compared to PIN.

REFRENCES

1. P. Aiyar Ramnath,*Advanced Law Lexicon,* (Nagpur; Wadhwa and Co;), 4th edition 2013 p 1561
2. Section 6 of Banking Regulation Act, 1949
3. Rajdeep and Joyteeta

4. A. French, "A case study on E-Banking security – When security becomes too sophisticated for the user to access their information", Journal of Internet Banking and Commerce, vol. 17, No. 2, pp. 1-14, August 2012.
5. Basel Committee on Banking Supervision Consultative Document Operational Risk, dated on January 31, 2001, http://www.bis.org/publ/bcbsca07.pdf
6. The Banking Law S.N Gupta, Universal Law Publication, 4th Edition.
7. RBI/2005-06/71 DBOD No. Comp.BC. 14/07.03.29/2005-06
8. RBI/2005-06/71 DBOD No. Comp.BC. 14/07.03.29/2005-06
9. Legal aspects of E-banking in India, https://www.scribd.com/document/267771691/Legal-aspects-of-E-banking-in-India
10. Negotiable instrument amendment act, 2002
11. Working Group on Internet Banking' to examine different aspects of Internet Banking (I-banking)

Cite this Article
Gunjan Bhagtani, Janvi Pandya. Contemporary Legal Issues in Indian E-Banking System. *Journal of Banking and Insurance Law.* 2019; 2(1): 17–24p.