ISSUES CONFRONTED BY INTERNET BANKING

Authors:
Dr. (Mrs.) Aditi A. Mahajan

Address for Correspondence:
Assistant Professor, Atharva Institute of Management Studies, Mumbai

ABSTRACT
Internet banking is a subject receiving great attention in the banking industry and the regulatory community. As with other areas of e-commerce, discussions about Internet banking often proceed without reference to the actual state of market developments. This paper describes the current state of Internet banking and discusses its implications for the banking industry and regulatory policy. Internet banking presents policy makers and regulatory authorities with a set of significant challenges. Internet banking has the potential to transform the banking business as it significantly lowers transaction and delivery cost.

INTRODUCTION
“Internet banking” refers to systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC) or other intelligent device.

Internet banking products and services can include wholesale products for corporate customers as well as retail and fiduciary products for consumers. Ultimately, the products and services obtained through Internet banking may mirror products and services offered through other bank delivery channels.

Internet banking is based on technology that by its very nature is designed to expand the “virtual” geographic reach of banks and customers without necessarily requiring a similar “physical” expansion. Such market expansion can extend beyond national borders which significantly increases cross-border cooperation challenges for bank supervisors due to the following factors:

1. The potential ease and speed with which banks located anywhere in the world can conduct activities with customers over interconnected electronic networks into countries where a bank is not licensed or supervised.

2. The potential ability of a bank or non-bank to use the Internet to cross borders and to seamlessly link banking activities that have typically been subject to supervision with non-banking activities that might be unsupervised by any financial market authority.

3. The practical difficulties faced by national authorities wishing to monitor or control local access to e-banking sites originating in other jurisdictions without the cooperation of home country authorities.

Banking organizations have been delivering services to consumers and businesses remotely for years. Electronic funds transfer, including small payments and corporate cash management systems, as well as publicly accessible machines for currency withdrawal and retail account management are global fixtures. However, delivering financial services over public networks such as the Internet is bringing about a fundamental shift in the financial services industry.

The changes created, and some of the technical characteristics of internet technology raise new concerns for both bankers and supervisors. Banking organizations are focusing increasingly on their e-banking activities and are globally expanding Internet banking activities, exploring the use of wireless networks and venturing into some new areas of electronic commerce.

Banks offer internet banking services to defend or expand market share or as a cost saving strategy to reduce paperwork and personnel. The Internet also provides banks with substantial opportunity to extend their customer reach beyond existing boundaries. However, the nature of the open network and the evolution of electronic commerce expose banks to significant competition from both banking and non-banking firms. In addition, electronic delivery channels operate in an uncertain legal and regulatory environment that differs by jurisdiction.

All these factors present new challenges for financial institutions in managing security, integrity and availability of services provided while remaining sufficiently profitable.

TECHNOLOGY AND SECURITY STANDARDS

The role of the network and database administrator is pivotal in securing the information system of any organization. Some of the important functions of the administrate via-vis system security are to ensure that only the latest versions of the licensed software with patches are installed in the system, proper user with access privileges are created and users are assigned appropriate groups as per their business roles, a proper system of back up of data and software in place and is strictly adhered to, business continuity plan is in place and frequently tested and there is a robust system of keeping log of all network activity and analyzing the same.

Organizations should make explicit security plant and document it. There should be a separate Security Officer/Group dealing exclusively with information systems security while the Commuter Security Officer will deal with its security. The Information Systems Audition will audit the information systems.
Access Control: Logical access controls should be implemented on data, systems application software, utilities telecommunication lines, libraries, system software, etc. Logical biometric technologies.

Firewalls: At the minimum, banks should use the proxy server types of firewall so that so 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 stateful inspection firewall is recommended which thoroughly inspects all packet of information, and past and present transactions are compared. These generally include real-time security alert.

Isolation of Dial up Services: The entire system 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.

Security Infrastructure: PKI is the most favored technology for secure Internet banking services. However, it is not yet commonly available. While PKI infrastructure is strongly recommended, during the transition period, unit IDRBT or Government puts in place the PKI infrastructure, the following options are recommended.

1. Usage of SSL, which ensures server authentication and the of client side certificates issued by the bank themselves using a certificate server.

2. The use of at least 128-bit SSL for securing browser to web server communication and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself.

Isolations of Application Servers: It is also recommended that all unnecessary services on the application server such as ftp, telnet should be disabled. The application server should be isolated from the e-mail server.

Security Log (audit Trail): All commuter accesses, including messages received, should be logged. All computer access and security violations (suspected or attempted) should be reported and follow up action taken as the organization’s escalation policy.

Penetration Testing: The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include the following.

1. Attempting to guess passwords using password-cracking tools.

2. Search for back door traps in the programs.

3. Attempt to overload the system using DDoS (Distributed Denial of Services) & DoS (Denial of Services) attacks.

4. Check if commonly known holes in the software, especially the browser and the e-mail software exist.

5. The penetration testing may also be carried out by engaging outside experts (often called ‘Ethical Hackers’)

**Physical Access Controls:** Though generally overlooked, physical access controls should be strictly enforced. The physical security should cover all the information systems and sites where they are housed both against internal and external threats.

**Backup and Recovery:** The bank should have a 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 having disaster recovery sites, where backed-up data is stored. These facilities should also be tested periodically.

**Monitoring against Threats:** The banks should acquire tool for monitoring system and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches.

**Education and Review:** The bank should review their security infrastructure and security policies regularly and optimize in the in the light of their own experiences and changing technologies. They should educate on a continuous basis their security personnel and also the end-users.

**Log of Messages:** The banking application run by the bank should have proper record keeping facilities for legal purposes. In may be necessary to keep all received and sent messages both is encrypted and decrypted form. (When stored in encrypted form, it should be possible to decrypt the information for legal purpose by obtaining keys with owners’ consent.)

**Certified products:** The banks should use those security solutions/products which are properly certified for security and for record keeping by independent agencies (such as IDRBT).

**Maintenance of Infrastructure:** Security infrastructure should be property tested before using the systems and applications for normal operations. The bank 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.

**Approval for i-banking:** All banks having operations in India and intending to offer Internet banking services to public must obtain an approval for the same form RBI. The application for approval should clearly cover the systems and products that the bank plans to use as well as the security plans and infrastructure it should include sufficient details for RBI to evaluate security, reliability, availability, auditability, recoverability, and other important aspects of the services.
RBI may provide model documents for Security Policy, Security Architecture, and Operations Manual.

**Legal Issues:** The banks providing Internet banking service, at present are only accepting request for opening of accounts. The accounts are opened only after proper physical introduction and verification. Considering the legal position prevalent, particularly of Section 131 of the Negotiable Instruments Act, 1881 and different case laws, the Group holds the view that there is an obligation on the banks not only to establish the identity but also to make enquires about integrity and reputation of the prospective customer. The Group, therefore, endorses the present practice but has suggested that after coming in to force of the Information Technology Act, 2000 and digital certification machinery being in place, it may be possible for the banks to rely on digital signature of the introducer. The present legal regime does not set out the parameters as to the extent to which a person can be bound respect of an electronic instruction purported to have been issued by him. Generally authentication is achieved by security procedure, which involves methods and devices like user-id password, personal identification number (PIN), code numbers and encryption etc., used to establish authenticity of an instruction. However, from a legal perspective a security procedure 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. This has raised the doubt whether the law would recognize the existing methods used by banks as valid methods of authentication. The Group holds the view that as in case of other countries, the law should be technology neutral.

In keeping with the view the law should be technology neutral, the Group has recommended that Section 3 (2) of the Information Technology Act, 2000 needs to be amended to provide that addition to the procedure prescribed there mutually agreed to by the concerned parties should be recognized as a valid method of authentication of an electronic document/ transaction during the transition period. Banks may be allowed to apply for a license to issue digital signature certificate under Section 21 of the Information Technology Act, 2000 and function as certifying authority for facilitating Internet banking. Reserve Bank of India may recommend to Central Government for notifying the business of certifying authority as an approved activity under clause (0) of Section 6(1) of the Banking Regulations Act, 1949.

Section 40A(3) of the Income Tax Act, 1961 recognizes only payments through a crossed cheque or crossed bank draft, where such payment exceeds Rs. 20,000, for the purpose of deductible expenses. Since the primary intention of the above provision, which is to prevent tax evasion by ensuring transfer of funds through identified accounts, is also satisfied in case of electronic transfer of funds between accounts, such transfers should also be recognized under the above provision. The Income Tax Act, 1961 should be amended suitably. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customer’s account. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors like customers not being careful about their passwords, PIN and other personal identification details and divulging the same to others, banks, sites being hacked despite all precautions and information accessed by inadvertent finders.

Banks offering Internet banking are taking all reasonable security measures like SSL access, 128 bit encryption, firewalls and other net security devices etc. The Group is of the view that despite
all reasonable precautions, bank will 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 risk. 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.

The banks providing Internet banking service and customers availing of the same are currently entering into agreements defining respective rights and liabilities in respect of Internet banking transaction. A standard format / minimum consent requirement to be adopted by banks may be designed by the Indian Banks’ Association, which should capture all essential conditions to be fulfilled by the banks, the customers and relative rights and liabilities arising there from. This will help in standardizing documentation as also develop standard practice among bankers offering Internet banking facility.

The concern that Internet banking transactions may become a conduit for money laundering has been addressed by the Group. Such transactions are initiated and concluded between designated accounts. Further, the proposed Prevention of Money Laundering Bill 1999 imposes obligation on every banking company to maintain records of transaction for certain prescribed period. The Banking Companies (period of Preservation of Records) Rules, 1985 also require banks to preserve certain records for a period ranging between 5 to 8 years. The Group is of the view that these legal provisions which are applicable to all banking transactions, whether Internet banking or traditional banking, will adequately take care of this concern and no specific measures for Internet banking is necessary.

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 customer availing of Internet banking services are being determined by bilateral agreements between the banks and customers. It is open to debate whether any bilateral agreement between the banks and customers. It is open to debate whether any bilateral agreement defining customers rights and liabilities, which are adverse to consumers than what is enjoyed by them in the traditional banking scenario will be legally tenable. Considering the banking practice and rights enjoyed by customers in traditional banking, it appears the banks providing Internet banking may not absolve themselves from liability to the customers on account of unauthorized transfer through hacking. Similar position may obtain in case of denial of service. Even though, The Information Technology Act, 2000 has provided for penalty for denial of access to a computer system (Section – 43) and hacking (Section 66), the liability of banks in such situations is not clear. The Group was of the view that the banks providing Internet banking may assess the risk and insure themselves against such risks.

The Information Technology Act, 2000, in Section 72 has provided for penalty for breach of privacy and confidentiality. Further, Section 79 of the Act has also provided for exclusion of liability of a network service provider for data traveling through their network subject to certain conditions. Thus, the liability of banks for breach of privacy when data is traveling through network is not clear. This aspect needs detailed legal examination. The issue of ownership of transactional data stored in banks’ computer systems also needs further examination.

### Internet Banking Risks

iJARS/Vol.1/ Issue I/Jun-Aug, 2012/146
Internet banking creates new risk control challenges for national banks. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank’s earnings or capital. The OCC has defined nine categories of risk for bank supervision purposes. The risks are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic, and reputation. These categories are not mutually exclusive and all of these risks are associated with Internet banking.

Credit Risk

Credit risk is the risk to earnings or capital arising from an obligor’s failure to meet the terms of any contract with the bank or otherwise to perform as agreed. Credit risk is found in all activities where success depends on counterparty, issuer, or borrower performance. It arises any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether on or off the bank’s balance sheet.

Internet banking provides the opportunity for banks to expand their geographic range. Customers can reach a given institution from literally anywhere in the World. In dealing with customers over the Internet, absent any personal contact, it is challenging for institutions to verify the bonafides of their customers, which is an important element in making sound credit decisions. Verifying collateral and perfecting security agreements also can be challenging with out-of-area borrowers. Unless properly managed, Internet banking could lead to a concentration in out-of-area credits or credits within a single industry. Moreover, the question of which state’s or country’s laws control an Internet relationship is still developing.

Interest Rate Risk

Interest rate risk is the risk to earnings or capital arising from movements in interest rates. From an economic perspective, a bank focuses on the sensitivity of the value of its assets, liabilities and revenues to changes in interest rates. Interest rate risk arises from differences between the timing of rate changes and the timing of cash flows (reprising risk); from changing rate relationships among different yield curves affecting bank activities (basis risk); from changing rate relationships across the spectrum of maturities (yield curve risk); and from interest-related options embedded in bank products (options risk). Evaluation of interest rate risk must consider the impact of complex, illiquid hedging strategies or products, and also the potential impact that changes in interest rates will have on fee income. In those situations where trading is separately managed, this refers to structural positions and not trading portfolios. Internet banking can attract deposits, loans, and other relationships from a larger pool of possible customers than other forms of marketing. Greater access to customers who primarily seek the best rate or term reinforces the need for managers to maintain appropriate asset/liability management systems, including the ability to react quickly to changing market conditions.

Liquidity Risk

Liquidity risk is the risk to earnings or capital arising from a bank’s inability to meet its obligations when they come due, without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned changes in funding sources. Liquidity risk also arises from the failure to recognize or address changes in market conditions affecting the ability of the bank to
liquidate assets quickly and with minimal loss in value. Internet banking can increase deposit volatility from customers who maintain accounts solely on the basis of rate or terms.

Conclusion

With the development of computer technology, the World Wide Web has become the connection medium for the networked world. Computers from locations that are geographically dispersed can talk with each other through the Internet. As with any new technology, there are positives and negatives associated with its use and Adoption. Finally, an e-marketplace can serve as an information agent that provides buyers and sellers with information on products and other participants in the market. Rapidly changing technology is continually bringing new goods and services to the market accompanied by new strategies to sell them. Therefore, it may also conclude that new ethical issues related to business will emerge. New ethical issues must be identified and immediate steps and actions should be taken.

REFERENCES:

- Economic law; 2001; pp.683-723.
- Diana Oblinger(2001); Will E-business Shape Andrew D. Mitchell(2001);Towards compatibility: The future of e-commerce within the global trading system; Journal of International the Future of Open and Distance Learning?; Open Learning; Vol. 16, No. 1, 2001; pp.9-25.
- Nir B. Kshetri (2001); Determinants of the Locus of Global E-commerce; Electronic Markets; Vol.11, No.4, 2001; pp.250-257.
- Patric Barwise(2001); TV, PC or Mobile? Future media for consumer e-commerce; Business strategy review; Vol.12, issue 1; 2001; pp.35-42.
- Richard T. Watson and George M. Zinkhan(1997); Electronic commerce strategy: addressing the key questions; Journal Of Strategic Marketing; Vol.5, pp.189-209.
- Young Jun Choi1, Chung Suk Suh(2005); The death of physical distance: An economic analysis of the emergence of electronic marketplaces; pp.597-614.