**ZENITH** International Journal of Business Economics & Management Research
Vol.2 Issue 5, May 2012, ISSN 2249 8826
Online available at http://zenithresearch.org.in/

# INTERNET BANKING: A STUDY OF REGULATORY, SUPERVISORY & MANAGEMENT ISSUES

**PROF. VIRENDER SINGH SOLANKI***

*Institute of Productivity & Management,
Meerut.

## ABSTRACT

With the popularity of PCs, easy access to Internet and World Wide Web (www), Internet is increasingly being used by banks as a channel for receiving instructions and delivering their products. Internet banking has grown at a very rapid pace, and many banks have made the development of services over the Internet a major component of their business and marketing strategy. From the perspective of banking, Internet banking is nothing more than traditional banking services delivered through an electronic communication backbone, via, Internet. But, in the process it has thrown open issues which have concerns beyond what a new delivery channel would normally bring and, hence, has compelled regulators world over to take note of this emerging channel. It has thrown challenges in the area of Legal issues relating to the jurisdiction of law, validity of electronic contract including the question of repudiation. The jurisdiction issue is whether to apply the law of the area where access to Internet has been made or where the transaction has finally taken place. Supervisory and operational issues like risk control measures, advance warning system, customer privacy, Information technology audit and re-engineering of operational procedures. Surveys done of bank supervisors conducted by the EBG (E-Banking Group) indicate that most respondents feel the need for additional, specialized supervisory guidance to address the issues and risks specifically posed by e-banking.

## INTRODUCTION

Continuing technological innovation and competition among existing banking organizations and new entrants have allowed for a much wider array of banking products and services to become accessible and delivered to retail and wholesale customers through an electronic distribution channel collectively referred to as e-banking. However, the rapid development of e-banking capabilities carries risks as well as benefits. Internet banking is a subject receiving great attention in the banking industry and the regulatory community.

Internet banking is growing at a fast speed, and many banks, including some of the nation's largest banks, have made the development of services over the Internet a major component of their business and marketing strategy. The range of products and services offered by different banks vary widely both in their content and sophistication.

## LEVELS AT WHICH INTERNET COULD BE USED IN BANKING SERVICES

Broadly, the banking services offered through INTERNET can be categorized into three types:

i. The Basic Level Service is the banks' websites which disseminate information on different products and services offered to customers and members of public in general. It may receive and reply to customers' queries through e-mail

ii. In the next level are Simple Transactional Websites which allow customers to submit their instructions, applications for different services, queries on their account balances, etc, but do not permit any fund-based transactions on their accounts.

iii. The third level of Internet banking services are offered by Fully Transactional Websites which allow the customers to operate on their accounts for transfer of funds, payment of different bills, subscribing to other products of the bank and to transact purchase and sale of securities, etc. Some of these banks are known as 'virtual' banks or 'Internet-only' banks and may not have any physical presence in a country despite offering different banking services. India does not allow purely virtual banks as of now.

It has thrown open issues which have concerns beyond what a new delivery channel would normally bring and, hence, has compelled regulators world over to take note of this emerging channel. Some of the distinctive features of i-banking are:

- It removes the traditional geographical barriers as it could reach out to customers of different countries / legal jurisdiction.
- 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.
- Security of banking transactions, validity of electronic contract, customers' privacy, etc., which have all along been concerns of both bankers and supervisors.
- 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.
- A new form of competition has emerged both from the existing players and new players of the market who are not strictly banks.

These concerns can be broadly addressed under three broad categories, viz.:-

**1. LEGAL AND REGULATORY ISSUE**: Legal issues cover those relating to the jurisdiction of law, validity of electronic contract including the question of repudiation, gaps in the legal / regulatory environment for electronic commerce. On the question of jurisdiction the issue is whether to apply the law of the area where access to Internet has been made or where the transaction has finally taken place. Allied to this is the question where the income has been generated and who should tax such income. There are still no definite answers to these issues.

**2. Security And Technology Issues**: Security of i-banking transactions is one of the most important areas of concerns to the regulators. Security issues include questions of adopting internationally accepted state-of-the art minimum technology standards for access control,

encryption / decryption (minimum key length etc), firewalls, verification of digital signature, Public Key Infrastructure (PKI) etc. The regulator is equally concerned about the security policy for the banking industry, security awareness and education.

**3. SUPERVISORY AND OPERATIONAL ISSUES:** The supervisory and operational issues include risk control measures, advance warning system, Information technology audit and re-engineering of operational procedures. The regulator would also be concerned with whether the nature of products and services offered are within the regulatory framework and whether the transactions do not camouflage money-laundering operations.

## THE STUDY

In the above background Reserve Bank of India constituted a Working Group to examine different issues relating to i-banking and recommend technology, security, legal and operational standards keeping in view the international best practices. The Group was headed by the Chief General Manager–in–Charge of the Department of Information Technology and comprised experts from the fields of banking regulation and supervision, commercial banking, law and technology. The Bank also constituted an Operational Group under its Executive Director comprising officers from different disciplines in the bank, who would guide implementation of the recommendations.

The Working Group, as its terms of reference, was to examine different aspects of Internet banking from regulatory and supervisory perspective and recommend appropriate standards for adoption in India, particularly with reference to the following:

1. Risks to the organization and banking system, associated with Internet banking and methods of adopting International best practices for managing such risks.

2. Identifying gaps in supervisory and legal framework with reference to the existing banking and financial regulations, IT regulations, tax laws, depositor protection, consumer protection, criminal laws, money laundering and other cross border issues and suggesting improvements in them.

3. Identifying international best practices on operational and internal control issues, and suggesting suitable ways for adopting the same in India.

4. Recommending minimum technology and security standards, in conformity with international standards and addressing issues like system vulnerability, digital signature, information system audit etc.

5. Clearing and settlement arrangement for electronic banking and electronic money transfer; linkages between i-banking and e-commerce

6. Any other matter, which the Working Group may think as of relevance to Internet banking in India

The Group held that i-banking did not mean any basic change in the nature of banking and the associated risks and returns. All the same, being a public domain and a highly cost effective delivery channel, it does impact both the dimension and magnitude of traditional banking risks. In fact, it adds new kinds of risk to banking. Some of the concerns of the Regulatory Authority in i-banking relate to technology standards including the level of security and uncertainties of legal jurisdiction etc. The Group decided to focus on above three major areas, where supervisory attention was needed. Accordingly, three sub-groups were formed for looking into three specific areas

1. Technology and Security Aspects,
2. Legal Aspects and
3. Regulatory and Supervisory Issues.

The Working Group had a number of deliberations. The views of the Group were crystallized in its report, which cover the following by way of its contents:

i. The basic structure of Internet and its characteristics

ii. International experience in i-banking, particularly with reference to USA, United Kingdom and other Scandinavian countries, who are pioneers in this form of banking.

iii. The Indian Scenario with reference to I-Banking.

iv. Different types of risks associated with banking in general and i-banking in particular.

v. Technology and security standards are discussed with emphasis on policy issues rather than on products and technical tools.

vi. The legal environment in which i-banking transactions are carried out is an important regulatory concern. The group has identified gaps in the existing framework and has suggested changes required.

vii. Operational aspects like internal control, early detection system, IT audit, technical manpower, etc are also discussed along with addressing the impact of i-banking on clearing and settlement arrangements.

viii. The specific recommendations of the group were given at the end of the report.

The report is thus a comprehensive document covering all aspects/considerations that should govern successful delivery of banking services through Internet. In this study the focus would be only on regulatory and supervisory issues.

## REGULATORY AND SUPERVISORY ISSUES

- Internet banking products – only licensed and supervised banks that have physical presence will be allowed to offer internet banking to the residents of India.

- Products only for account holders (intra bank- core banking and inter bank- through EFT/RBI fund transfer outside India not allowed).
- Service to include local currency products.
- Overseas branches of Indian Banks can offer internet banking to their overseas customers subject to regulations of the host country

**SUBJECT TO THE ABOVE, BANKS TO FOLLOW THE FOLLOWING INSTRUCTIONS**

- Banks to submit a security policy covering the recommendations made in the circular.
- Certificate from an independent auditor.
- RBI to be informed of any material change in the services/products offered.
- Every breach to be reported to RBI – may decide to commission special audit/inspection.
- Guidelines of 1998 on risk and controls in computers and telecom – applicable to internet banking.
- Banks to develop clear outsourcing guidelines to manage risk out of third party service providers such as disruption of service, defective service or personal gaining knowledge of banks systems.
- Mandatory disclosure of risk , liability and responsibilities of customers in doing business through internet
- Banks should also provide the latest published financial results over the net.
- Hyperlinks from bank's websites to other must be confined to those with which bank has payment arrangement or sites of their subsidiaries /principals so that banks do not sponsor products unrelated to banking.

**AUTHORIZATION AND REGULATORY ISSUES**

Although banks are already providing services cross-border in the physical world (through mail for instance), Internet related technologies significantly increase the potential for jurisdictional ambiguities with respect to the supervisory responsibilities of different national authorities. Such situations could lead to insufficient supervision of cross-border e-banking activities. Additionally, non-banks may offer with greater facility bank-like services without any type of supervisory approval or oversight due to definitional ambiguities that may exist with regard to what constitutes a bank (or banking services).

Furthermore, banks may inadvertently engage in cross-border activities without knowledge of local limitations. Such situations may expose banks to heightened legal risk associated with non-

compliance with different national laws and regulations, including those pertaining to authorization, consumer protection, record-keeping and reporting requirements, and anti money laundering.

## PRUDENTIAL SUPERVISION

While the existing solvency requirements and prudential supervision rules apply equally to e-banking and traditional banking activities, alternative electronic delivery channels raise prudential issues that must be viewed in a new light by supervisors. These include the oversight of outsourcing and partnership arrangements, and the oversight of security and data integrity controls and safeguards, especially when the supporting operations are located in another jurisdiction.

Similar to the situation regarding e-banking authorization and regulatory issues, additional complexities and ambiguities exist with respect to cross-border home and host supervisory relationships. The existing Basel Committee guidance provides a firm foundation for supervising cross-border banking activities but the EBG (Electronic Banking Group) recognizes that it needs to be reviewed to assure that it is sufficiently robust for the e-banking world.



## CROSS-BORDER E-BANKING ISSUES

A framework to deal with e-banking issues among supervisors is essential to effective cross-border supervision, although the specifics may differ between jurisdictions depending upon a variety of local factors. Supervisors will have different perspectives in developing such a framework depending on whether they are a home country supervisor, a host country supervisor, or as is frequently seen, both. Two cross-border scenarios reflect the differences in perspective that need to be examined:

1. In-country institutions providing banking services to customers outside the home country (the in-out scenario).

2. Institutions based outside the home country providing banking services to parties within the home country (the out-in scenario). This scenario has two subsets: one where the banking institution has a physical presence and licensed operations within the host country (physical out-in); and one where the banking institution has no physical presence and/or license and the banking services are solely provided in a "virtual" manner (virtual out-in).

## THESE ISSUES CAN BE CLUBBED INTO THE FOLLOWING FOUR TYPES

### 1. OPERATIONAL RISK ISSUES

The open architecture of the Internet exposes the banks' systems to decide access through the easy availability of technology. The dependence of banks on third party providers places knowledge of banks' systems in a public domain and leaves the banks dependent upon relatively small firms which have high turnover of personnel. Further, there is absence of conventional audit trails as also relative anonymity of transactions due to remote access. It is imperative that

security and integrity of the transactions are protected so that the potentiality for loss arising out of criminal activities, such as fraud, money laundering, tax evasion etc. and a disruption in delivery systems either by accident or by design are mitigated. The supervisory responses to manage operational risk matters include issue of appropriate guidance on the risk (including outsourcing risk) control and record maintenance, issue of minimum standards of technology and security appropriate to the conduct of transactional business, extension of 'know your Customer' rules for transactions on the Internet, and insistence on appropriate and visible disclosure to inform customers of the risks that they face on doing business on the Internet.

## 2. CROSS BORDER ISSUES

The Internet knows no frontiers, and banks can source deposits from jurisdiction where they are not licensed or supervised or have access to payment systems. Customers can potentially park their funds in jurisdictions where their national authorities have no access to records. The issues of jurisdiction, territoriality and recourse become even more blurred in the case of virtual banks. Cross border issues would also come into play where banks choose to locate their processing centers, records or back up centers in different jurisdictions. While country - specific approaches are being adopted at the national level, the 'Group on e-banking' set up by the Basle Committee on Banking Supervision (BCBS) is engaged in bringing about harmonization in approaches at an international level.

## 3. CUSTOMER PROTECTION AND CONFIDENTIALITY ISSUES

The loss of customer confidentiality may pose a reputation risk to banks and the banking system as a whole. Transacting business on the Internet exposes data being sent across the Internet to interception by unauthorized agents, who may then use the data without the approval of the customers. There has also been incidence where glitches have developed in web sites permitting customers to access each other's accounts. To address these risks, customers need to be educated through adequate disclosures of such risks.

## 4. COMPETITIVENESS AND PROFITABILITY ISSUES

While Internet banking is expected to substantially reduce the cost of doing transactions in the long run, the limited business being done on the Internet has yet to pay for the infrastructure in which banks have invested. This includes the tie up with technology companies in setting up payment gateways, portals and Internet solutions and the alliance with other businesses for cross-selling products. The coming years may however see a scenario where the margins of conventional banks come under pressure because of competition from Internet banking, including virtual banks, which need no infrastructure expenses. These issues have to be kept in mind by supervisors while deciding their approach to e-banking.

## COMMITTEES ON RISK MANAGEMENT

The Basel Committee for Banking Supervision (BCBS) has constituted an Electronic Banking Group (EBG) to develop guiding principles for the prudent risk management of e-banking activities as an extension of the existing Basel Committee Risk Management Principles. The Group identified the areas of concern for supervision of cross border e-banking activities and

promoted cooperative international efforts within the banking industry. It evolved sound practices and encouraged and facilitated exchange of information, training material, guidance etc., developed by other members and supervisors around the world. Therefore, there is a need for continued interaction among the central banks and supervisors with a view to enhancing the abilities of the supervisory community to keep pace with the dynamic e-banking activities. This Working Group, therefore, recommends that the Reserve Bank of India should maintain close contact with regulating / supervisory authorities of different countries as well as with the Electronic Banking Group of BCBS and review its regulatory framework in keeping with developments elsewhere in the world.

The Basel Committee has issued a number of papers addressing sound supervisory practices for "home" and "host" country banking supervisors including guidance on effective cross border communication and coordination. These papers serve as a basic reference for bank supervisory and other financial market authorities in all countries. They establish several key cross-border principles pertaining to (i) global consolidated supervision; (ii) contact and information exchange with host country supervisory authorities; (iii) and supervision of local operations of foreign banks.



The Basel Committee guidance has provided comfort to host-country supervisors that cross border branches and subsidiaries licensed and supervised within their borders are capably supervised by the parent bank's home-country supervisor. However, many cross-border issues arise from the rapid expansion of e-banking activities that were not contemplated when the Basel Committee's existing guidance was developed.

E-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 increase cross-border cooperation challenges for bank supervisors due to:

(i) 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.

(ii) 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.

(iii) 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.

## THE TARAPORE COMMITTEE REPORT ON E-BANKING

The Tarapore Committee is in agreement that Basel-II norms would strengthen the banking system, and improve its overall accountability. Its recommendations on bank-specific approach to risk management, and institutional neutrality in the context of regulatory arbitrage are noteworthy.

The Tarapore Committee recommendations on strengthening the banking system in India are in consonance with the Basel-II requirements. A significant recommendation made by the Tarapore Committee is on regulatory arbitrage. It recommended that regulation should be institution neutral. If not, there could be distortions in the market, which would encourage the flow of business to areas where there is laxity of regulation. This could pose a risk to the system. Although RBI is alive to the issue, it would take time to put this into practice. Overall, efforts are on to configure systems to check market distortions.

The Narasimham Committee had already recommended strengthening of the banking sector through consolidation. The prime mover for bank mergers is the requirement of a minimum cash adequacy ratio (CAR) of nine percent, and minimum capital of Rs. 300 crores. Although the Committee recommendations were primarily directed at public sector banks, private sector banks have been more active in achieving mergers.

The system of bank supervision has been revamped along (CAMELS) capital adequacy, asset quality, management, earnings, liquidity, systems and control, besides risk management. Further, considerable convergence has been achieved in the definition of non-performing assets (NPAs) among banks, RBI, and the auditors.



## SUPERVISORY APPROACH

There is no doubt about the challenges faced by Regulators in developing guidelines for the effective supervision of Internet banking activities. As a minimum, Supervisors should be able to determine if the bank's board of directors has adopted effective policies for Internet banking that are consistent with safe and sound banking practices and are appropriate to the size of the bank and the nature and scope of its operations. In order to determine the soundness of those policies and procedures the following are some of the issues, which may be reviewed with the bank:

The business plan, including the time table for the launch of the internet service, the types of Products and services that would be included and expected volume of transactions that would be conducted through the internet.

The contractual arrangements for liability arising from unauthorized or fraudulent transactions.

The security arrangements for the system, in particular, what security measures have been/will be installed to:

- Restrict access to those users who are authorized to access.
- Authenticate the identity and authority of the parties concerned to ensure the enforceability of transactions conducted through the internet.
- Maintain the secrecy of information while it is in passage over the communications network.
- Ensure that the data has not been modified accidentally or fraudulently whilst in the passage on the communication network.

- Prevent unauthorized access to the institution's central computer system and data base.
- The procedures and safeguards for monitoring unusual transactions, detection and investigation of possible fraud.
- Any limit on the amount of transactions or any restrictions on the types of transfer that can be conducted through the internet.
- Whether the various security aspects of the system (including encryption/fire wall/authentication techniques) have been reviewed by qualified independent consultants;
- What arrangements are in place to ensure that the risk management systems and internal controls are reviewed and evaluated on a regular basis (e.g. by external or internal auditors);
- What is the contingency plan for major breaches in the security of the system including recovery procedures, damage controls procedures and safeguarding the interests of customers;
- Whether the bank's management and personnel display acceptable knowledge and technical skills to manage Internet banking, given the size and complexity of the bank.

## BROAD REGULATORY FRAMEWORK

There are four key tools that regulators need to focus on to address the new challenges posed by the arrival of Internet Banking.

**1. ADAPTATION:** In light of how rapidly technology is changing and what the changes mean for banking activities, keeping regulations up to date has been, and continues to be, a far-reaching, time-consuming, and complex task. In May 2001, the Bank for International Settlements issued its "Risk Management Principles for Electronic Banking," which discusses how to extend, adapt, and tailor the existing risk-management framework to the electronic banking setting. For example, it recommends that a bank's board of directors and senior management review and approve the key aspects of the security control process, which should include measures to authenticate the identity and authorization of customers, promote non-repudiation of transactions, protect data integrity, and ensure segregation of duties within E-banking systems, databases, and applications. Regulators and supervisors must also ensure that their staffs have the relevant technological expertise to assess potential changes in risks, which may require significant investment in training in hardware and software.

**2.LGALIZATIONE:** New methods for conducting transactions, new instruments, and new service providers will require legal definition, recognition, and permission. For example, it will be essential to define an electronic signature and give it the same legal status as the handwritten signature. Existing legal definitions and permissions, such as the legal definition of a bank and the concept of a national border, will also need to be re-thought.

**3. HARMONIZATION:** International harmonization of electronic banking regulation must be a top priority. This means intensifying cross-border cooperation between supervisors and coordinating laws and regulatory practices internationally and domestically across different regulatory agencies. The problem of jurisdiction that arises from "borderless" transactions is, as of this writing, in limbo. For now, each country must decide who has jurisdiction over electronic banking involving its citizens. The task of international harmonization and cooperation can be viewed as the most daunting in addressing the challenges of electronic banking.

**4. INTEGRATION:** This is the process of including information technology issues and their accompanying operational risks in bank supervisors' safety and soundness evaluations. In addition to the issues of privacy and security, for example, bank examiners will want to know how well the bank's management has elaborated its business plan for electronic banking.

## LEGISLATIVE BACKGROUND IN INDIA

The Basel Committee on Banking Supervision, which is a committee of banking supervisory authorities of G-10 countries, has been in the forefront of the international attempt in the development of standards and the establishment of a framework for bank supervision towards strengthening international financial stability. In 1997, in consultation with the supervisory authorities of a few non G-10 countries including India, it drew up the 25 “Core Principles for Effective Banking Supervision” which were in the nature of minimum requirements intended to guide supervisory authorities which were seeking to “strengthen their current supervisory regime”.

Being one of the central banks which was involved in the exercise of drawing up the Core Principles, the Reserve Bank of India had assessed its own position with respect to these Principles in 1998. The assessment had shown that most of the Core Principles were already enshrined in our existing legislation or current regulations. Gaps had been identified between existing practice and principle mainly in the areas of risk management in banks, inter-agency cooperation with other domestic/international regulators and consolidated supervision. Internal working groups were set up to suggest measures to bridge these gaps and their recommendations were accepted by the Board for Financial Supervision and implemented in due course.

Given the spread and reach of the Indian banking system, with over 60,000 branches of more than 100 banks, implementation is a challenge for the supervisors. However, the Reserve Bank of India is committed to the full implementation of the Core Principles. The Bank also serves on the Core Principles Liaison Group of the BCBS, which has been formed “to promote the timely and complete implementation of these principles worldwide”.

## NEED FOR THE ACT

Further when a need was felt for An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of

India Act, 1934 and for matters connected therewith or incidental thereto. This was done by the government by implementing Information Technology Act 2000. Many a things were resolved, but as the subject is continuously evolving, a need was felt for amendment and the Government came out with the amendments in the form of Information Technology Act 2008.

## THE IN-OUT SCENARIO

When banking organizations provide e-banking services in foreign countries, mutual understanding of the oversight process by both the home and host supervisors is required. Existing Basel Committee guidance clearly establishes the principle that the home country supervisor is responsible for oversight of the banking organization on a consolidated basis and the host supervisor's oversight is limited to the organization's activities conducted within its local market.

## THE OUT-IN SCENARIO

In the "physical out-in" scenario, the foreign institution typically has both (i) some type of licensed physical presence in the host's jurisdiction that is overseen by the host banking supervisor and (ii) access to the local payments system. In this scenario, the host supervisor will apply its normal supervisory oversight processes to the local institution with a focus on activities within its local market. To the extent that e-banking regulatory issues are identified, they would be addressed locally with the licensed entity and communicated to the home country supervisor as warranted, where necessary, cooperative supervisory action involving both the host and home supervisors would be undertaken.

## CURRENT SITUATION

Surveys done of bank supervisors conducted by the EBG (E-Banking Group) indicate that supervisors generally believe that their existing laws, prudential bank regulations, and supervisory policies apply to e-banking activities. However, most respondents note the need for additional, specialized supervisory guidance to address the issues and risks specifically posed by e-banking. The EBG has determined that almost all banks are currently taking a conservative approach to entering new cross-border markets; essentially following the existing procedures that they have used when entering a new foreign market that requires formal regulatory approval. To date, banks have generally refrained from conducting e-banking services in foreign markets where they do not already transact such services through traditional "brick and mortar" distribution channels (e.g. licensed branches, agencies or subsidiaries). Banks that currently conduct cross-border e-banking activities have limited such activities to either their home country currency or the currency of a country in which they are already licensed and have access to the local currency settlement systems either directly or indirectly through a licensed physical presence in the country.

It could also result in banks conducting cross-border e-banking without the benefit of a sound understanding of local customs, market conventions, regulations and legal requirements.

In addition, unlicensed and/or unsupervised financial institutions may not exercise the same degree of prudential restraint and control as supervised banks when rolling out cross-border

activities. This situation could result in unlicensed institutions providing, via the Internet, banking-like services into jurisdictions where banks are not permitted to provide the same service(s).

A threefold challenge results for banking supervisors:

(i) Supervisors need to recognize that the Internet allows for the provision of e-banking services that can span geographic borders and potentially call into question existing jurisdictional authorization requirements and the regulatory processes;

(ii) Supervisors need to recognize the implications of taking a restrictive approach toward currently regulated banks without an even-handed treatment of foreign organizations that may conduct identical or nearly identical activities via the Internet in the local jurisdiction;

(iii) Supervisors should ensure that banks appropriately manage the legal uncertainty during the period while the legal infrastructure for cross-border e-banking remains under construction.

## MAJOR FINDINGS & IMPLICATIONS

a) There are serious issues of jurisdiction as internet knows no frontiers, and banks can source deposits from jurisdiction where they are not licensed or supervised or have access to payment systems.

b) On the question of jurisdiction the issue is whether to apply the law of the area where access to Internet has been made or where the transaction has finally taken place. Allied to this is the question where the income has been generated and who should tax such income. There are still no definite answers to these issues.

c) Non-banks may offer with greater facility bank-like services without any type of supervisory approval or oversight due to definitional ambiguities that may exist with regard to what constitutes a bank or banking services.

d) Only licensed and supervised banks that have physical presence will be allowed to offer internet banking to the residents of India.

e) The dependence of banks on third party providers places knowledge of banks' systems in a public domain and leaves the banks dependent upon relatively small firms which have high turnover of personnel.

f) While Internet banking is expected to substantially reduce the cost of doing transactions in the long run, the limited business being done on the Internet has yet to pay for the infrastructure in which banks have invested.

## BIBLIOGRAPHY


- Malhotra, P. and Singh, B. (2006, October–December) 'The impact of internet banking on bank's performance: the Indian experience', South Asian Journal of Management, Vol.13,No. 4.
- Malhotra, P. and Singh, B. (2007) 'Determinants of internet banking adoption by banks in India', Internet Research, Vol. 17, No. 3.
- Palsokar P. V. (2000). Electronic Banking IBA Bulletin, March.
- Rao, G. R. and Prathima, K. (2003) 'Internet Banking in India', Mondaq Business Briefing, 11 April.
- Reserve Bank of India (2001), Report on Internet Banking, at www.rbi.org.in.
- Agarwal, N., Agarwal, R., Sharma, P. and Sherry, A. M. (2003), E banking for comprehensive E Democracy: An Indian Discernment, Journal of Internet Banking and Commerce, Vol. 8, No. 1, June, 2003.
- Arunachalam, L.and Sivasubramanian, M. (2007) 'The future of Internet Banking in India', Academic Open Internet Journal, Vol. 20. Available online at: www.acadjournal.com
- Dasgupta, P. (2002), Future of E " banking in India, available at www.projectshub.com
- Ganesan R,and Vivekanandan K, (2009) 'A secured hybrid architecture model for internet banking (e-banking)'. Journal of Internet banking and commerce, April, vol.14, no.1.