CHAPTER – VII

INFORMATION TECHNOLOGY AND FINANCIAL SYSTEM OF BANKS IN INDIA.

1. INFORMATION TECHNOLOGY IN BANKING SYSTEM OF INDIA.
2. E-BANKING AND RBI.
3. REGULATORY AND SUPERVISORY POLICIES FOR BANKS.
4. ELECTRONIC BANKING: CHALLENGES AND CONCERNS
5. ELECTRONIC MONEY (E-MONEY)
6. E-SECURITY IN INDIAN BANKING.
7. CURRENT ISSUES IN INDIAN BANKING.
1. INFORMATION TECHNOLOGY IN BANKING SYSTEM OF INDIA

Information technology (IT) has transformed the functioning of businesses, the world over. It has bridged the gaps in terms of the reach and the coverage of systems and enabled better decision-making based on latest and accurate information, reduced costs and overall improvement in efficiency. In the Indian context, the financial sector, especially the banking sector, has been a major beneficiary from the inroads made by IT. Many new processes, products and services offered by banks and other financial intermediaries are now IT-centred. Effective integration of technology with sound business practices requires business process re-engineering and banks in India need to follow up on the beginnings made in this regard. Newer delivery channels to customers – Automated Teller Machines (ATMs), and the networking of ATMs in the form of Shared Payment Networks, Internet Banking – and implementation of Core Banking solutions by most banks are some examples.

The RBI has played a proactive role in the implementation of IT in the banking sector. IT based initiatives are focused on meeting the three pronged objective of better house keeping, improved customer service
and overall systemic efficiency. The RBI has come out with a financial sector Technology Vision Document outlining the approach to be followed for IT implementation for the medium-term period of about three years. This document will help banks in finalizing their IT plans in tandem with the overall approach for the banking sector, as envisioned by the RBI.

**E-Banking:**

Electronic banking (E-Banking is a generic term encompassing internet banking, telephone banking, mobile banking etc. In other words, it is a process of delivery of banking services and products through electronic channels such as telephone, internet, cell phone etc. The concept and scope of E-Banking is still evolving.

Several initiatives taken by the Government of India as well as the Reserve Bank of India (RBI) have facilitated the development of e-banking in India. As a regulator and supervisor, the RBI has made considerable progress in consolidating the existing payment and settlement systems, and in upgrading technology with a view to establishing an efficient, integrated and secure system functioning in a real-time environment, which has further helped the development of e-banking in India. The Government of India enacted the IT Act, 2002 with effect from October 17, 2000, which provides legal recognition to electronic transactions and other means of electronic commerce.

Finland was the first country in the world to have taken a lead in e-banking. The Scandinavian countries have the largest number of Internet

---

38 Jhori and Hauhari, Role of Computers in Banking Operation System (New Delhi, Himalaya Publication House), 1994
users, with up to one-third of bank customers in Finland and Sweden taking advantage of e-banking. Internet banking is also widespread in Austria, Korea, Singapore, Spain, Switzerland, etc. E-banking facilities an effective payment and accounting system thereby enhancing the speed of delivery of banking services considerably. While the e-banking has improved efficiency and convenience, it has also posed several challenges to the regulators and supervisors.

In response to the challenges thrown by the Internet banking, regulators and supervisors from various countries have prepared their own mechanism of regulation. There is a matrix of legislation and regulations within the United States that specifically codifies the use of and rights associated with the internet and e-commerce, in general, and electronic banking and internet banking activities, in particular. The concerns of the Federal Reserve are limited to ensuring that Internet banking and other electronic banking services are implemented with proper attention to security, safety and soundness of the bank, and the protection of the banks’ customers.

In the U.K, there is no specific legislation for regulating e-banking activities. The FSA is neutral on regulations of electronic banking. In Sweden, no formal guidance has been given to examiners by the sveriges Bank on e-banking. General guidance has been apply equally to Internet banking activities. The role of the Bank of Finland has been, as part of general oversight of financial market in Finland, mainly to monitor the ongoing development of Internet banking without active participation. The Reserve Bank of New Zealand applies the same approach to the regulation of both Internet banking activities and traditional banking activities. There are however, banking activities and traditional banking
activities. There are however, banking regulations that apply only to Internet banking. Supervision is based on public disclosure of information rather than application of detailed prudential rules.

The monetary Authority of Singapore (MAS) subjects Internet banking to the same prudential standards as traditional banking. The MAS drafted an ‘Internet banking Technology Risk management Guidelines’ in September 2002, which calls upon all banks providing Internet banking to establish a sound and robust risk management process. The Hong Kong regulatory approach towards e-banking is less specific in nature. The Hong Kong Monetary Authority (HKMA) expects their banks to undertake a rigorous analysis of the security aspects of their system by getting it reviewed by qualified independent experts.

Like many of these countries, India does not have specific regulatory laws for e-banking. The existing regulatory framework over banks has been extended to Internet banking as well. However, certain guidelines have been issued to banks to recognize the risks arising from electronic modes and to devise control mechanisms that are needed to mitigate such risks. Banks offering the e-banking services in India need to comply with the guidelines.

2. **E-BANKING AND RBI**:⁴⁰

The RBI has been gearing up to grading itself as a regulator and supervisor of the technologically dominated financial system. In 1998, it availed the technical assistance project of Department for International Development (DFID), UK for upgrading its supervisory system and

---

⁴⁰ Indian Banking and E-Banking, RBI Bulletin, November 2004
adaptation of its supervisory functions to the computerized environment. It issued guidelines on ‘risks and control in computer and telecommunication system’ in February 1998 to all the banks advising them to evaluate the risks inherent in the systems and put in place adequate control mechanisms to address these risks, which can be broadly put under three heads, viz, IT environment risks, IT operations risks and product risks.

The existing regulatory framework over banks has also been extended to internet banking. These guidelines cover various issues that would fall within the framework of technology, security standards and legal and regulatory issues. Virtual banks, which have no officers and function only on line are not permitted to offer e-banking services in India and that only banks licensed under the Banking Regulation Act and having a physical presence in India are allowed to offer such services. Further, banks are required to report to the RBI every branch if failure of security systems and procedures in Internet Banking, while the RBI at its direction may decide to commission special audit/inspection of such banks.

As per cent guidelines, banks no longer need any prior approval of the Reserve Bank for offering the internet banking services. Nevertheless, banks must have their internet policy and they need to ensure that it is in line with parameters as set by the Working Group on Internet Banking in India (2001). The main recommendations of this Working Group are set forth below.

Main Recommendations of the Working Group on Internet Banking (Chairman: S.R. Mittal), 2001
Reserve bank of India constituted a Working Group to examine different issues relating to internet banking and recommend technology, security, legal standards 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 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 India.

Keeping in view the term of reference, the group made a number of recommendations. A summary of this recommendation is given below.

**Technology and Security Standard:** 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 administrator via-a-system security are to ensure that only the latest versions of the licensed software with latest patches are installed in the system, proper user groups with access privileges are created and users are assigned to appropriate groups as per their business roles, a proper system of back up of data and software is in place and is strictly adhered to, system of keeping log of all network activity and analyzing the same.

Organizations should make explicit security plan and document it. There should be a separate security Officer/Group dealing exclusively with information systems security. The Information Technology Division will actually implement the computer systems while the Computer Security Officer will deal with its security. The Information Systems Auditor 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 access control techniques may include user-ids, passwords, smart cards or other biometric technologies.
**Firewalls:** 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 stateful 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.

**Isolation of Dial up Services:** 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.

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

1. Usage of SSL, which ensures server authentication and the use of client certificates issued by the banks themselves using a Certificate Server.

2. 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.

**Isolation 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 computer 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 Service) & DoS (Denial of Service) 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 Hacker’).

**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.

**Back up 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 tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches.

**Education and Review:** 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 on a continuous basis their security personnel and also the end-users.

**Log of Messages:** The banking applications run by the bank 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. (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 only 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 properly 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 from 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, audit ability, 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 services, at present are only accepting the 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 lows, the Group holds the view that there is an obligation on the banks not only to establish the identify but also to make enquiries 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 in 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, and 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 section3 (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 that 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 in addition to the procedure prescribed there in or that may be prescribed by the Central government, a security procedure mutually agreed 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 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 (o) 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 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, banks will be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of services 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 is respect of Internet banking transactions. 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 transactions 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 customers 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 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 I-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 the computer system (Section-43) and hacking (Section66), 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 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.

3. REGULATORY AND SUPERVISORY POLICIES FOR BANKS

All banks, which propose to offer transactional services on the internet, should obtain approval from RBI prior to commencing these services. Banks’ application for such permissions should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners and third party service providers and system and control procedures the bank proposes to adopt for managing risks, etc. The bank should also submit a security policy covering recommendations made in chapter-6 of this report and a certificate from a independent auditor that the minimum requirements prescribed there have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services/products offered by them.

RBI may require banks to periodically obtain certificates from specialist external auditors certifying their security control and procedures. The banks will report to RBI every breach or failure of
security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks.

To a large extent the supervisory concerns on Internet banking are the same as those of electronic banking in general. The guidelines issued by RBI on ‘Risks and Controls in Computers and Telecommunications’ will equally apply to Internet banking. The RBI as supervisor would cover the entire risks associated with electronic banking as a part of its regular inspections of banks and develop the requisite expertise for such inspections. Till such capability is built up, RBI may outsource this function to qualified EDP auditors.

Record maintenance and their availability for inspection and audit is a major supervisory focus. RBI’s guidelines on ‘Preservation and Record Maintenance’ will need to be updated to include access to electronic record only by authorized officials, regular archiving of data, a sufficiently senior officer to be in charge of archived data with well defined responsibilities, use of proper software platform and tools to prevent unauthorized alternation of archived data, availability of data on-line, etc. If not available on-line, the system should be capable of making available the data for the same financial year within 24 hours and past data within a period of maximum 48 hours.

Banks should develop outsourcing guidelines to manage effectively, risks arising out of third party service providers such as risks of disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks’ systems and misutilizing the same, etc. Alternatively, IBA or IDBRT may develop broad guidelines for use of the banking community.
With the increasing popularity of e-commerce, i.e., buying and selling over the Internet, it has become imperative to set up ‘Inter-bank Payment gateways’ for settlement of such transactions. The Group have suggested a protocol for transactions between the customer, the bank and the portal and have recommended a framework for setting up of payment gateways. In their capacity as regulator of banks and payment systems of the country, the RBI should formulate norms for eligibility of an institution to set up a payment gateway and the eligible institutions should seek RBI’s approval for setting up the same.

Only institutions who are members of the cheques clearing system in the country may be permitted to participate in Inter-bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Only direct debits and credits to accounts maintained with the participating banks by parties to an e-commerce transaction may be routed through a payment gateway. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intr-bank payments (i.e. transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway.

Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as possible, in real time. It must be obligatory for payment gateways to maintain complete trace of any payment transaction covering such details like date and time. It must be obligatory for payment gateways to maintain complete trace of any payment transaction covering such details like date and time of origin of transaction, payee, payer and a unique transaction reference number (TRN).
Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated using user-id and password. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL/128 bit encryption must be used as minimum level of security. Adequate firewalls and related security measures must be taken to ensure privacy to the participating institutions in a payment gateway. Internationally accepted standards such as ISO8583 must be used for transmitting payment and settlement messages over the network.

The RBI may have a panel of auditors who will be required to certify the security of the entire infrastructure both at the payment gateway end and the participating institutions end prior to making the facility available for customers use. The credit risk associated with each payment transaction will be on the payee bank. The legal basis for such transactions and settlement will be the bilateral contracts between the payee and payee’s bank, the participating banks and service provider and the banks themselves. The rights and obligations of each party must be clearly stated in the mandate and should be valid in a court of law. It will be necessary to make customers aware of risks inherent in doing business over the Internet. This requirement will be met by making mandatory disclosures of risks, responsibilities and liabilities to the customers through a disclosure template. The banks should also provide their latest published financial results over the net.

Hyperlinks from bank’s websites often raise the issue of reputational risk. Such links should not mislead the customers in to
believing that they sponsor any particular product or any business unrelated to banking. Hence, hyperlinks to bank’s website from different portals are normally meant to pass information pertaining to purchases made by bank’s customers in the portal. Banks must follow the minimum recommended security precautions while dealing with such request, which includes customer authentication through user-id and password, independent confirmation of transaction by the customer and authorizing payment, use of SSL and 128 bit encryption for all communication both with the portal and customer browser terminal, etc.

On the question of additional capital charge on banks, which undertake Internet banking, the group held the view that standards have not yet been developed for measuring additional capital charge for operational risk. However, this requirement could be covered as the RBI moves towards risk based supervision.

The applicability of various existing laws and banking practices to e-banking is not tested and is still in the process of evolving, both in India and abroad. With rapid changes in technology and innovation in the field of e-banking, there is a need for constant review of different laws relating to banking and commerce. The Group, therefore, recommends that the Reserve Bank of India may constitute a multi disciplinary high level standing committee to review the legal and technological requirements of e-banking on continual basis and recommend appropriate measures as and when necessary.

The regulatory and supervisory framework for e-banking is continuing to evolve and the regulatory authorities all over the world recognize the need for cooperative approach in this area. 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. 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 Group submitted its report in June 2001 and the Reserve Bank while accepting the recommendations of the Working Group, issued guidelines on ‘Internet Banking in India’ for implementation by banks. It also stated that the earlier guidelines issued by the Reserve Bank on ‘Risks and Controls in Computers and Telecommunications’ (1998) would equally apply to Internet banking as well.

4. **E-BANKING: CHALLENGES AND CONCERNS**

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 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 4 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 e-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 exposes 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.

1. A significant increase in competition in the electronic financial services industry as both banking and non-banking firms rapidly introduce new financial products and services.
2. Rapid technological improvements in telecommunications and computer hardware and software enabling greater speed in transactions processing.
3. Bank management and staff often lack expertise in technology and e-banking risk issues.
4. Greater reliance on outsourcing to third party service providers, and a proliferation of new alliances and joint ventures with non-financial firms.
5. Greater demand for global infrastructures for technology that are scalable flexible and interoperable, both within and across enterprises and that can ensure the security, integrity and availability of information and services.
6. Increased potential for fraud, due to the absence of standard business practices for customer verification and authentication on open networks like the Internet.
7. Legal and regulatory ambiguity and uncertainty with respect to the application and jurisdiction of current laws and regulations to evolving e-banking activities.
8. The collection, storage and frequent sharing of significant quantities of customer data can lead to customer privacy issues that potentially create prudential risks for banks (e.g. legal and reputational).

9. Questions regarding the effectiveness and efficiency of online disclosures. Lengthy or complicated online disclosures may cause customers to simply “click through” or even quit a web site; moreover, extensive disclosure reduces the speed at which web sites and pages can be downloaded.

Banks and bank supervisors generally agree that the supervisory principles that apply to traditional banking are applicable to e-banking. However, the combination of rapid changes in technology and the degree of bank dependence on technology vendors and service providers modify and sometimes magnify traditional risks. Hence, there is a need for additional supervisory guidance in selected areas to enhance the overall risk management framework for e-banking activities.

These developments in e-banking to date suggest the following.

1. The desire to benefit from the advantages of e-commerce in financial services has become widespread. The financial services industry is increasingly focused on providing technology-based financial services solutions directly to customers in order to help build and retain customer bases.

2. Speed-to-market has become a critical factor for success in e-banking. To reduce time to market, banking institutions are allying with non-banking firms to provide total financial services solutions.
3. The current trends in the formation of strategic alliances and technology outsourcing will grow.

These developments present challenges for both banks and bank supervisors. Bank management needs to re-evaluate the robustness of traditional risk management practices in light of the new risks posed by e-banking activities. Also, bank supervisors need to take a balanced approach to the introduction of new regulation and supervisory policy on e-banking, so as to ensure safe and sound operations of banks while at the same time not stifling innovation and the competitiveness of the banks relative to non-banks.

5. **ELECTRONIC MONEY (E-MONEY)**

In recent years, there has been a gradual switchover from the use of paper-based payments media to those based on electronics. While the basic characteristics of these new instruments are by and large similar to those of paper-based instruments, the former present a different set of challenges to policy makers. Electronic money (e-money) is one such new product which has appeared on Indian horizon recently.

**A. Meaning of E-Money:** E-money may be broadly defined as an electronic store of monetary value on a technical device used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument. These products could be classified into two broad categories, viz. (a) pre-paid stored value card (sometimes called “electronic purse”) and (b) per-paid software based product that uses computer networks such as internet (sometimes referred to as “digital cash” or “network

---

41 Indian Banking and E-Security, RBI Bulletin, 2004
money”). The stored value card scheme typically uses a microprocessor chip embedded in a plastic card while software based scheme typically used specialized software installed in a personal computer.

**B. Recommendations of the Working Group on Electronic Money (Chairman : Zaire J. Camas), 2002**

In January 2002, the RBI constituted a Working Group of Electronic Money which submitted its report in July 2002. The Group identified certain areas of concern from the point of view of the central bank in the context of more widespread use of e-money so that the conduct of monetary policy is not impaired and at the same time, the integrity of the instrument is also preserved. Some of the suggestions made by the Group included (a) multi-purpose e-money to be issued only by authorized banks on a credit basis, which should be strictly regulated and closely monitored, (b) ensure redeem ability in order to preserve the unit of account function of money as well as to control money supply in the economy and (c) reporting of monetary statistics for the purposes of monetary policy and protection against criminal abuse, such as money laundering.

Summary and recommendations of the Report are set forth below. Broadly, e-money is an electronic store of monetary value on a technical device. E-money could be classified as (a) pre-paid stored value card (sometimes called “electronic purse”) and (b) pre-paid software based product that uses computer networks such as internet (sometimes referred to as “digital cash” or “network money”). The stored value card could be

---

42. Jhori and Hauhari, Role of Computers in Banking Operation System (New Delhi, Himalaya Publication House), 1994
of three types – single purpose card. The single-purpose card generally with a magnetic chip recording the amount of fund therein is designed to facilitate only one type of transaction e.g., telephone calls, public transportation, laundry, parking facilities (acceptor) are identical for such cards. The closed-system or the limited-purpose cards as generally used in a small number of well-identified points of sale within a well-identified location such as corporate/university campus. The multipurpose card on the other can perform variety of functions with several vendors viz., credit card, debit card, stored value card, identification card, repository of personal medical information etc.

While it may not be desirable place any limit on storing monetary value in e-money, it is expected that e-money could be used to substitute central bank notes regulatory oversight, restrictions on issuers and their implications for monetary policy is extremely critical from the point of view of the central bank.

After considering various issues, the Group recommends that multi-purpose e-money may be permitted to be issued only against payment of full value of central bank money or against credit only by the banks. The issuance of e-money on credit basis should, however, be strictly regulated and closely monitored.

It needs to be appreciated that issuers must be under obligation to offer redemption of their e-money liabilities net of service charges, if so required. From monetary policy point of view, such redemption requirement is essential in order to preserve unit of account function of money as also to control money supply in the economy.
With regard to status of issuers of e-money, it may be indicated that there are five reasons which may warrant banks as the issuers of multi-purpose e-money.

These include attributes of e-money being close to demand liabilities of the bank, implications of e-money on velocity of circulation of money and its corresponding impact on monetary statistics, the option to impose reserve requirement on e-money, the need for closure monitoring of e-money when these would be issued as credit and the technical security of e-money. For all these reasons, the Group recommends that only banks should be allowed to issue multipurpose e-money. However, single-purpose and limited-purpose e-money should be allowed to be issued by any entity including banks.

Non-banks should be not be permitted to issue multi-purpose e-money. If they are permitted, they along with banks must conform to seven minimum prudential requirements as laid down by European Central Bank (ECB) in 1998. These are (i) prudential supervision of issuers of e-money by the central bank, (ii) solid and transparent legal arrangements codifying the rights and obligations of issuers, merchants, consumers and the regulators, (iii) adequate technical, organizational money, (iv) protection against criminal abuse, (v) supplying of all relevant information to the central bank for the purpose of monetary policy, (vi) legal obligations to redeem e-money against central bank money at par at the request of the holder and (vii) the right of the central bank to impose reserve requirement on issuers of e-money.

E-money could have profound impact on compilation of monetary statistics and money supply unless regulated prudently. E-money could be issued against cash (i.e., 100 per cent backed by central bank money
paid upfront). Since e-money are close substitutes of central bank money, these should be explicitly accounted for in monetary statistics. If e-money, is allowed to be issued only by banks, then currency would be substituted with demand/time liabilities through e-money. In that eventually, issuance of e-money would be money stock neutral and no change would be required in the definition of money stock. However, if e-money is issued by entities other than depository institutions (i.e., banks), the money creating sector as embedded in compilation of monetary statistics would need to be broadened.

There could be a situation where residents could use e-money supplied by entities outside the country for domestic transactions. In that case, monetary aggregates would lose its predictive power.

It is expected that the proportion of interest bearing liabilities in monetary aggregates would grow in the event of growing use of e-money which would render them more unstable, and information content of monetary aggregates would also change.

If e-money is issued on credit, there is a possibility that the issuers may assume a leveraged position. There is, therefore, a need for continuous monitoring of the behaviour of issuing authorities for balanced growth of their assets and liabilities, particularly liabilities arising out of issuance of e-money. For these reasons, the Group recommends that the central bank should regulate and closely monitor the practice of issuing e-money on credit.

If consumes prefer to use e-money vis-à-vis currency, then for a given stock of currency, the money multiplier would go up which would in turn increase the aggregate money supply in the economy more than what would have been case without e-money. Also with large scale use
of e-money, it has been apprehended that central bank’s balance sheet may shrink to such an extent relative to that of the banking sector that it may be unable to perform its liquidity absorption function on account of non-availability of adequate volume of assets. Apart from constraining its liquidity management function, relative shrinkage in balance sheet may also have serious implications regarding loss of seigniorage revenue for the central bank. As a counter argument, it is maintained that there should always be a lower bound below which the use of currency notes and coins should not go down so that there should also be a limit below which reserve money should not shrink relative to broad money stock.

A review of developments indicate that while considerations of potential benefits of micro-economic efficiency, extension of banking to urban poor and increasingly private provision of payment and settlement services in the economy in future, macro-economic stabilizations policy warrants that there should be a case for public regulation over such provision. Also, currency uses are characterized by network externalities in that larger the number of users, larger is the settlement value of the currency concerned implying that currency could at best be supplied oligopolistically. There are, in fact, the fundamental reasons for which the “monopoly right” in the issuance of currency should be in the hands of some public authority, preferably the central bank. Even then, there cannot be any final judgment on this issue at this point of time. In view of all these considerations, the Group, therefore, recommends that the RBI should regularly monitor closely all these developments so that integrity of the financial system is preserved.

The RBI should also periodically review issues relating to legal framework, if any, technical security and the clearing and settlement
arrangements of different e-money schemes and the practices of various e-money schemes, both in India and abroad, for preserving integrity of the financial market. On the issue whether entities other than the central bank could issue independent media of exchanges, the Group feels that such a possibility is apparently remote in India at this point of time. However, RBI may continually keep track of these developments for smooth functioning of the financial market.

6. E-SECURITY IN INDIAN BANKS

No innovation is without challenges and IT is no exception to this rule. The most prominent challenge arising from these innovations relates to the concept of security (Mohan, 2004c). Considering the scope for fraud in the e-banking area and the possibility of contagion, the Reserve Bank as regulator and supervisor has been proactive in addressing the risks associated with e-banking that could have otherwise undermined the credibility of the India banking sector. The Reserve Bank has been promptly addressing issues related to fraud with the use of electronic banking facility. Even after issuing guidelines for a secured e-banking, the Reserve Bank from time to time advises the banks on control mechanisms to plug the loopholes and the same was also communicated to other banks so that they remained vigilant and control the misuse of internet banking system.

In India, the legal infrastructure of promoting e-banking has not yet been put in place in a comprehensive manner. India does not have a licensed certifying authority appointed by the Controller of Certifying

---

43 Indian Banking and E-Security, RBI Bulletin, December 2004
Authorities to issue digital signature certificates. Also, India is not yet a signatory to the International Cyber nations for exchanging information concerning crime and cyber criminals. Further, there are unresolved legislative issues related to cyber crimes laws, clarification relating to regulatory authority over e-money products, consumer protection and privacy laws. To make the e-banking operations in India more widespread, secure and efficient, these issues need to be addressed by relevant authorities.

As the banking practices and legislations concerning e-banking are still in the process of evolution in India and abroad because of technological innovations, there is a need for a constant review of various legislations and regulatory framework relating to banking and commerce. The Reserve Bank is monitoring and reviewing the legal and other requirements of e-banking on a continuous basis to ensure that the e-banking would develop on sound lines and the e-banking related challenges would not pose a threat to financial stability.

Reviewing the technological development in Indian commercial banks, the Economic Survey, 2006-07 observed. “The banking sector in India is adapting itself to rapid innovations in technology particularly on the information-based technology front to impart efficiency in providing wide range of products and services to the public at large. Computerization of banking operations had received high importance in 2005-06. Since September 1999 to March 2006. PSBs incurred an expenditure of Rs. 10|676 crore on computerization and development of communication networks. Out of 27 PSBs branches of as many as 10 PSBs were 100 per cent computerized, while more than 50 per cent branches of 12 banks were computerized by end-March 2006.
The number of branches providing ‘core banking solutions’ (CBS) in recent years is increasing rapidly. Under CBS, a number of services are being provided such as ‘anywhere banking’, ‘everywhere access’, and quick transfer to funds in an efficient manner and at reasonable cost. New private sector banks, foreign banks and a few old private sector banks have already put in place CBS; PSBs are increasingly adopting similar system. The total number of branches of PSBs offering CBS increased from 11.0 per cent as on March 31, 2005 to 28.0 per cent as on March 31, 2006.

Total number of Automated Teller Machines (ATMs) installed by the banks were 21,147 at end-march 2006. Nationalized banks with 7,165 ATMs, were the largest providers of the ATM service followed by new private banks (6,112), SBI group (5,443), old private banks (1,547) and foreign banks (88). [20]

7. CURRENT ISSUES IN INDIAN BANKING

Despite substantial improvements in the banking sector, some issues have to be addressed over time as the reform process is entrenched further. The discussion on banking developments revolves around on a wide range of issues including the following.

1. Overall redrawing of boundaries between the State ownership of financial entities and private sector ones.
2. Public sector character of the banking sector and efficiency.
4. Corporate governance in banks and other segments of the financial system.

5. Transparency of policies and practices of monetary and financial agencies and accountability.

6. Prudential requirements of market participants together with comprehensive and efficient oversight of the financial system.

7. Maintenance of best practices in accounting and auditing, as also collection, processing and dissemination of symmetric and detailed information to meet the market needs.

8. Relevance of Development Finance Institutions (DFIs).

The commonality among these concerns has given rise to a wide recognition and acceptance of having a set of international standards and best practices that every systemically important country should strive to foster and implement.

Financial sector reforms, introduced in the early 1990s ion a gradual and sequenced manner, were directed at the removal of various deficiencies from which the system was suffering. The basic objectives of reforms were to make the system more stable and efficient so that it could contribute in accelerating the growth process.

In response to reforms, the Indian banking sector has undergone radical transformation during the 1990s. Reforms have altered the organizational structure, ownership pattern and domain of operations of institutions and infused competition in the financial sector. The competition has forced the institutions to repositions in the financial sector. The competition has forced the institutions to reposition themselves in order to survive and grow. The extensive progress in technology has enabled markets to graduate from outdated systems to modern market design, thus, bringing about a significant reduction in the speed of expectation of trades and transaction costs.
With the increasing integration of various segments of financial markets, the distinctions between banks and other financial intermediaries are also getting increasingly blurred. Another important aspect of reforms in the financial sector has been the increased participation of financial institutions, especially banks, in financial institutions and markets. While increased inter-linkages are expected to lead to increased efficiency in the resource allocation process and the effectiveness of monetary policy, they also increases the risk of contagion from one segment of another with implications for overall financial stability. This would call for appropriate policy responses during times of crisis. Increased inter-linkages also raise the issue of appropriate supervisory framework.

Banking sector reforms in India are grounded in the belief that competitive efficiency in the real sectors of the economy will not realise its full potential unless the banking sector was reformed as well. Thus, the principal objective of banking sector reforms was to improve the allocate efficiency of resources and accelerate the growth process of the real sector by removing structural deficiencies affecting the performance of banks.

In India, while the banking system continues to play a predominant role, it is significant to note that, as a result of various reform measures, the relative stability of the financial markets has increased. This augurs well for the overall stability of the financial system. The East Asian crisis has also underlined the need for a balanced financial system wherein financial markets also play an important role in providing necessary liquidity, especially during times of crisis. Banking system also requires liquidity in times of stress, which only deep and liquid financial markets can provide.