Report on Internet Banking

Chapter–1– Introduction

1.1 Background

1.1.1 Banks have traditionally been in the forefront of harnessing technology to improve their products, services and efficiency. They have, over a long time, been using electronic and telecommunication networks for delivering a wide range of value added products and services. The delivery channels include direct dial – up connections, private networks, public networks etc and the devices include telephone, Personal Computers including the Automated Teller Machines, etc. With the popularity of PCs, easy access to Internet and World Wide Web (WWW), Internet is increasingly used by banks as a channel for receiving instructions and delivering their products and services to their customers. This form of banking is generally referred to as Internet Banking, although the range of products and services offered by different banks vary widely both in their content and sophistication.

1.1.2 Broadly, the levels of banking services offered through INTERNET can be categorized in to 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. The above forms of Internet banking services are offered by traditional banks, as an additional method of serving the customer or by new banks, who deliver banking services primarily through Internet or other electronic delivery channels as the value added services. 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.

1.1.3 From the perspective of banking products and services being offered through Internet, Internet banking is nothing more than traditional banking services delivered through an electronic communication backbone, viz, Internet. But, in the process it has thrown open issues which have ramifications beyond what a new delivery channel would normally envisage and, hence, has compelled regulators world over to take note of this emerging channel. Some of the distinctive features of i-banking are:

1. It removes the traditional geographical barriers as it could reach out to customers of different countries / legal jurisdiction. This has raised the question of jurisdiction of law / supervisory system to which such transactions should be subjected,
2. It has added a new dimension to different kinds of risks traditionally associated with banking, heightening some of them and throwing new risk control challenges,
3. Security of banking transactions, validity of electronic contract, customers' privacy, etc., which have all along been concerns of both bankers and supervisors have assumed different dimensions given that Internet is a public domain, not subject to control by any single authority or group of users,
4. 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,

5. A new form of competition has emerged both from the existing players and new players of the market who are not strictly banks.

1.1.4 The Regulatory and Supervisory concerns in i-banking arise mainly out of the distinctive features outlined above. These concerns can be broadly addressed under three broad categories, viz, (i) Legal and regulatory issues, (ii) Security and technology issues and (iii) Supervisory and operational issues. 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.

1.1.5 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.

1.1.6 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.

1.1.7 The Central Bank may have its concern about the impact of Internet banking on its monetary and credit policies. As long as Internet is used only as a medium for delivery of banking services and facilitator of normal payment transactions, perhaps, it may not impact monetary policy. However, when it assumes a stage where private sector initiative produces electronic substitution of money like e-cheque, account based cards and digital coins, its likely impact on monetary system can not be overlooked. Even countries where i-banking has been quite developed, its impact on monetary policy has not been significant. In India, such concern, for the present is not addressed as the Internet banking is still in its formative stage.

1.1.8 The world over, central bankers and regulators have been addressing themselves to meet the new challenges thrown open by this form of banking. Several studies have pointed to the fact that the cost of delivery of banking service through Internet is several times less than the traditional delivery methods. This alone is enough reason for banks to flock to Internet and to deliver more and more of their services through Internet and as soon as possible. Not adopting this new technology in time has the risk of banks getting edged out of competition. In such a scenario, the thrust of regulatory thinking has been to ensure that while the banks remain efficient and cost effective, they must be aware of the risks involved and have proper built-in safeguards, machinery and systems to manage the emerging risks. It is not enough for banks to have systems in place, but the systems must be constantly upgraded to changing and well-tested technologies, which is a much bigger challenge. The other aspect is to provide conducive regulatory environment for orderly growth of such form of banking. Central Banks of many countries have put in place broad regulatory framework for i-banking.

1.1.9 In India, too i-banking has taken roots. A number of banks have set up banking portals allowing their customers to access facilities like obtaining information, querying on their accounts, etc. Soon, still higher level of online services will be made available. Other banks will sooner than later, take to Internet banking. The Indian scenario is discussed in detail in Chapter-4 of this report.

1.2 Constitution of the Working Group

1.2.1 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 standards and operational standards keeping in view the international best practices. The Group is 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 composition of both the Groups is at Annexure-2 and

Annexure-3.

1.2.2 Terms of reference

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.

1.3. Approach of the Group:

1.3.1 The first meeting of the Working Group was held on July 19, 2000. It was decided that members of both Working Group and Operational Group would participate in all meetings and deliberations. The Group, in its first meeting identified the broad parameters within which it would focus its deliberations.

1.3.2 The Group agreed that Internet banking is a part of the electronic banking (e-banking), the main difference being that in i-banking the delivery channel was Internet, a public domain. Although the concerns of e-banking and i-banking have many things in common, the fact that Internet is a public domain called for additional security measures. It was agreed that the Group would primarily focus its attention on I - banking and to the extent there were commonality between i-banking and e-banking, its recommendation would also apply to e-banking.

1.3.3 The Group further 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. Its cost effective character provides opportunities for efficient delivery of banking services and higher profitability and a threat to those who fail to harness it.

1.3.4 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: (i) technology and security aspects, (ii) legal aspects and (iii) regulatory and supervisory issues. The sub-groups could seek help of external experts in the relevant fields, if needed.

1.4 Layout of the Report:

1.4.1. The views of the Group were crystallized after several rounds of deliberations of members of both the Working Group and the Operational Group. The reports prepared by the three sub-groups were discussed and assimilated in to this report. The report is presented in nine chapters. Chapter–1, the introductory chapter, gives the background leading to the formation of the Group, its composition, terms of reference and the approach adopted by the Group in finalizing its recommendations.

1.4.2. The basic structure of Internet and its characteristics are described in Chapter–2 in order to explain the nature of concerns addressed in the chapters to follow. Also explained in the chapter is the growth of Internet banking and different products and different e-commerce concepts.

1.4.3. Chapter–3 describes International experience in i-banking, particularly with reference to USA, United Kingdom and other Scandinavian countries, who are pioneers in this form of banking. Chapter- 4 looks at the Indian scenario as it prevails now.

1.4.4. Chapter–5 discusses different types of risks associated with banking in general and i-banking in particular. Emphasis is given on normal risks associated with banking which gets accentuated when the services are delivered through Internet. Risks relating to money laundering and other cross border transactions are discussed.

1.4.5. Technology and security standards are core concerns for Regulatory Authorities in relation to Internet banking. A separate sub-group looked in to these issues, which are discussed in detail in Chapter–6. Emphasis is given on technology and security standards and policy issues rather than on products and technical tools.

1.4.6 Another important regulatory concern is the legal environment in which i-banking transactions are carried out. It is of importance to identify gaps in the existing framework and to suggest changes required. The legal sub-group had made a detailed analysis of legal questions involved, which are discussed in Chapter – 7.

1.4.7 Chapter–8 deals with various control measures required to be adopted by banks to manage risks discussed in earlier chapters. Operational aspects like internal control, early detection system, IT audit, technical manpower, etc are also discussed. The impact of i-banking on clearing and settlement arrangements has also been addressed. The sub-group on Regulatory and Supervisory issues had addressed the above questions.

1.4.8 Chapter–9 contains recommendations of the Working Group. Shri S. H. Bhojani had disagreement with some of the observations / recommendations by the Group and a note of dissent is appended as Annexure-1.

1.5. Acknowledgement

1.5.1 The group wishes to acknowledge and put on record its appreciation of support received from various quarters in completing the Report.

1.5.2 The Central Banks and Regulatory Authorities of different countries and the Bank for International Settlement were approached for papers compiled by them on the subject and for details of regulations already in place. All relevant materials were received from them promptly. The Group gratefully acknowledges their support and cooperation.

1.5.3 Shri Girish Vaidya of Infosys technologies Ltd. had made an erudite presentation on Internet Banking to the Group, which was very useful in finalizing this report. The Group gratefully acknowledges his efforts.

1.5.4 Three sub-groups were formed to focus deliberations on three important aspects of

Internet banking. These sub-groups utilized the expertise of professionals / bankers in finalizing their views. The convenors and members of sub-groups worked most diligently to produce reports of very high quality. The Group gratefully thanks them for their efforts. The Group gratefully acknowledges the contributions made by S/Shri G. Subba Rao, Head, Internal Audit , ABN Amro Bank, Shri P. C Narayan, Executive Vice President, Global Trust Bank and Shri Sasidharan Menon , Head, Internal Audit , Deutsche Bank as members of sub-group on Regulatory and Supervisory Issues.

1.5.5 The Department of Banking Operations and Development provided secretarial service to the Working Group. The Group wishes to put on record its appreciation of efforts put in by the secretarial team consisting of DGMs (Shri SR. Das, Shri Arnab Roy), AGM (Shri Indrajit Roy) and Managers (Shri Chetan N Balwir, Dr. T K Karthykeyan, Shri JP Bansal) in organizing the meetings, arranging the background papers and drafting of the Report.

1.5.6 The Group wishes to place on record its appreciation of contributions made by all members of the Operational Group who participated in the deliberations and offered their valuable suggestions and guidance.

1.5.7 The Member-secretary of the Working Group, Shri M. P. Kothari, worked with utmost zeal in ensuring smooth conduct of the entire process right from the inception of the Working Group till the finalization of the Report. The Group gratefully acknowledges his efforts, but for which the Report would not have been completed.

Chapter–2– Internet Banking - a new medium

2.1 Internet – its basic structure and topology

2.1.1 Internet is a vast network of individual computers and computer networks connected to and communicate with each other using the same communication protocol – TCP/IP (Transmission Control Protocol / Internet Protocol). When two or more computers are connected a network is created; connecting two or more networks create 'inter-network' or Internet. The Internet, as commonly understood, is the largest example of such a system. Internet is often and aptly described as 'Information Superhighway', a means to reach innumerable potential destinations. The destination can be any one of the connected networks and host computers.

2.1.2 Internet has evolved to its present state out of a US Department of Defence project ARPANet (Advanced Research Project Administration Network), developed in the late 1960s and early 1970s as an experiment in wide area networking. A major perceived advantage of ARPANet was that the network would continue to operate even if a segment of it is lost or destroyed since its operation did not depend on operation of any single computer. Though originally designed as a defence network, over the years it was used predominantly in areas of scientific research and communication. By the 1980s, it moved out of Pentagon's control and more independent networks from US and outside got connected to it. In 1986, the US National Science Foundation (NSF) established a national network based on ARPA protocol using commercial telephone lines for connectivity. The NSFNet was accessible by a much larger scientific community, commercial networks and general users and the number of host computers grew rapidly. Eventually, NSFNet became the framework of today's Internet. ARPANet was officially decommissioned in 1990.

2.1.3 It has become possible for innumerable computers operating on different platforms to communicate with each other over Internet because they adopt the same communication protocol, viz, TCP/IP. The latter, which stands for 'Transmission Control Protocol / Internet Protocol', is a set of rules which define how computers communicate with each other. In order to access Internet one must have an account in a host computer, set up by any one of the ISPs (Internet Service Providers). The accounts can be SLIP (Serial Line Internet Protocol) or PPP (Point to Point Protocol) account. These accounts allow creating temporary TCP/IP sessions with the host, thereby allowing the computer to join the Internet and directly establish communication with any other computer in the Internet. Through this type of connection, the client computer does not merely act as a remote terminal of the host, but can run whatever programs are available on the web. It can also run several programs simultaneously, subject to limitations of speed and memory of the client computer and modem. TCP/IP protocol uses a unique addressing scheme through which each computer on the network is identified.

2.1.4 TCP / IP protocol is insecure because data packets flowing through TCP / IP networks are not normally encrypted. Thus, any one who interrupts communication between two machines will have a clear view of the data, passwords and the like. This has been addressed through Secured Socket Layer(SSL), a Transport Layer Security (TLS) system which involves an encrypted session between the client browser and the web server.

2.1.5 FTP or File Transfer Protocol is a mechanism for transferring files between computers on the Internet. It is possible to transfer a file to and from a computer (ftp site) without having an account in that machine. Any organization intending to make available to public its documents would normally set up a ftp site from which any one can access the documents for download. Certain ftp sites are available to validated users with an account ID and password.

2.1.6 *e-mail:* The most common and basic use of Internet is the exchange of e-mail (electronic mail). It is an extremely powerful and revolutionary result of Internet, which has facilitated almost instantaneous communication with people in any part of the globe. With enhancements like attachment of documents, audio, video and voice mail, this segment of Internet is fast expanding as the most used communication medium for the whole world. Many websites offer e-mail as a free facility to individuals. Many corporates have interfaced their private networks with Internet in order to make their e-mail accessible from outside their corporate network.

2.1.7 *World Wide Web (WWW)*

2.1.7.1 Internet encompasses any electronic communication between computers using TCP/IP protocol, such as e-mail, file transfers etc. WWW is a segment of Internet, which uses Hyper Text Markup Language (HTML) to link together files containing text, rich text, sound, graphics, video etc. and offers a very convenient means of navigating through the net. It uses hypertext transfer protocol (HTTP) for communication between computers. Web documents, which are referred to as pages, can contain links to other related documents and so on, in a tree like structure. The person browsing one document can access any other linked page. The web documents and the web browsers which are the application programs to access them, are designed to be platform independent. Thus any web document can be accessed irrespective of the platform of the computer accessing the document and that of the host computer. The programming capabilities and platform independence of Java and Java applets have further enriched the web. The 'point and click' method of browsing is extremely simple for any lay user of the net. In fact, the introduction of web since early 1990 has made Internet an extremely popular medium and its use in business has been enhanced dramatically.

2.1.7.2 The next in the HTML genre is the Extensible Markup Language (XML), which allows automated two-way information flow between data stores and browser screens. XML documents provide both the raw content of data and the data structure and is projected by its proponents as taking the web technology beyond the limits of HTML.

2.1.8 *Wireless Application Protocol (WAP):*

WAP is the latest industry standard which provides wireless access to Internet through handheld devices like a cellular telephone. This is an open standard promoted by WAP forum and has been adopted by world's all major handset manufacturers. WAP is supplemented by Wireless Application Environment (WAE), which provides industry wise standard for developing applications and services for wireless communication networks. This is based on WWW technology and provides for application for small screens, with interactive capabilities and adequate security. Wireless Transaction Protocol (WTP), which is the equivalent of TCP, sets the communication rules and Wireless Transport Layer Security (WTLS) provides the required security by encrypting all the session data. WAP is set to revolutionize the commercial use of net.

2.1.9 *Security:*

One of the biggest attractions of Internet as an electronic medium is its openness and freedom. It is a public domain and there is no restriction on who can use it as long as one adheres to its technical parameters. This has also given rise to concerns over the security of data and information transfer and privacy. These concerns are common to any network including closed user group networks. But over the Internet, the dimensions of risk are larger while the control measures are relatively fewer. These issues are discussed in detail in Chapter–5 and Chapter–6 of the report. It will be sufficient to say here that the key components of such concern are, (i) authentication, viz., assurance of identity of the person in a deal, (ii) authorization, viz., a party doing a transaction is authorized to do so, (iii) the privacy or confidentiality of data, information relating to any deal, (iv) data integrity, viz., assurance that the data has not been altered and (v) non repudiation, viz., a party to the deal can not deny that it originated the communication or data.

2.2 E-Commerce:

2.2.1 Even though started as network primarily for use by researchers in defence and scientific community, with the introduction of WWW in early 1990s, use of Internet for commerce has grown tremendously. E-commerce involves individuals and business organizations exchanging business information and instructions over electronic media using computers, telephones and other telecommunication equipments. Such form of doing business has been in existence ever since electronic mode of data / information exchange was developed, but its scope was limited only as a medium of exchange of information between entities with a pre-established contractual relationship. However, Internet has changed the approach to e-commerce; it is no longer the same business with an additional channel for information exchange, but one with new strategy and models.

2.2.2 A business model generally focuses on (i) where the business operates, that is, the market, the competitors and the customers, (ii) what it sells, that is, its products and services (iii) the channels of distribution, that is, the medium for sale and distribution of its products and (iv) the sources of revenue and expenditure and how these are affected. Internet has influenced all the four components of business model and thus has come to influence the business strategy in a profound way. The size of the market has grown enormously as technically, one can access the products and services from any part of the world. So does the potential competition. The methods of reaching out to customers, receiving the response and offering services have a new, simpler and efficient alternative, now, that is, Internet. The cost of advertisement, offer and delivery of services through Internet has reduced considerably, forcing most companies to rework their strategies to remain in competition.

2.2.3 A research note by Paul Timmers of European commission had identified eleven business models, which have been commercially implemented. These are e-shop, e-procurement, e-auction, e-mall, Third-party market place, Virtual communities, Value chain service providers, Value chain integrators, Collaboration platforms and Information brokers. He classified business models along two dimensions, i.e, degree of innovation and extent of integration of functions. The innovation ranged from the electronic version of a traditional way of doing business (e-shop) to more innovative ways by offering functions that did not exist before. The second dimension, i.e, extent of integration ranges from a single function business model (like e-shop) to fully integrated functionality (value chain integrator). In the top end of the graph are models, which cannot be implemented in a traditional way and are critically dependent upon information technology and creating value from information flow. Business models, in between these two limits are a combination of both dimensions in different degrees and have some degree of analogy in traditional firms.

2.2.4 There are two types of e-commerce ventures in operation: the old brick and mortar companies, who have adopted electronic medium, particularly Internet, to enhance their existing products and services, and / or to offer new products and services and the pure e-ventures who have no visible physical presence. This difference has wider ramifications than mere visibility when it comes to issues like customer’s trust, brand equity, ability to service the customers, adopting new business culture and cost. These aspects of e-commerce will be touched upon in the following discussions.

2.2.5 Another way of classifying the e-commerce is by the targeted counterpart of a business, viz, whether the counterpart is a final consumer or another business in the distribution chain. Accordingly, the two broad categories are: Business-to-Consumer (B2C) and

Business-to-Business (B2B).

2.2.6 *Business-to-Consumers (B2C):*

2.2.6.1 In the B2C category are included single e-shops, shopping malls, e-broking, e-auction, e-banking, service providers like travel related services, financial services etc., education, entertainment and any other form of business targeted at the final consumer. Some of the features, opportunities and concerns common to this category of business irrespective of the business segment, are the following.

2.2.6.2 *Opportunities:*

2.2.6.2.1 Internet provides an ever-growing market both in terms of number of potential customers and geographical reach. Technological development has made access to Internet both cheaper and faster. More and more people across the globe are accessing the net either through PCs or other devices. The purchasing power and need for quality service of this segment of consumers are considerable. Anybody accessing Internet is a potential customer irrespective of his or her location. Thus, any business targeting final consumers cannot ignore the business potential of Internet.

2.2.6.2.2 Internet offers a unique opportunity to register business presence in a global market. Its effectiveness in disseminating information about one's business at a relatively cost effective manner is tremendous. Time sensitive information can be updated faster than any other media. A properly designed website can convey a more accurate and focussed image of a product or service than any other media. Use of multimedia capabilities, i.e., sound, picture, movies etc., has made Internet as an ideal medium for information dissemination. However, help of other media is necessary to draw the potential customers to the web site.

2.2.6.2.3 The quality of service is a key feature of any e-commerce venture. The ability to sell one's product at anytime and anywhere to the satisfaction of customers is essential for e-business to succeed. Internet offers such opportunity, since the business presence is not restricted by time zone and geographical limitations. Replying to customers' queries through e-mail, setting up (Frequently Asked Questions) FAQ pages for anticipated queries, offering interactive help line, accepting customers' complaints online 24 hours a day and attending to the same, etc. are some of the features of e-business which enhance the quality of service to the customers. It is of crucial importance for an e-venture to realize that just as it is easier to approach a customer through Internet, it is equally easy to lose him. The customer has the same facility to move over to another site.

2.2.6.2.4 Cost is an important issue in an e-venture. It is generally accepted that the cost of overhead, servicing and distribution, etc. through Internet is less compared to the traditional way of doing business. Although the magnitude of difference varies depending on the type of business and the estimates made, but there is unanimity that Internet provides a substantial cost advantage and this, in fact, is one of the major driving forces for more number of traditional business adopting to e-commerce and pure e-commerce firms to sprout.

2.2.6.2.5 Cost of communication through WWW is the least compared to any other medium. Many a time one's presence in the web may bring in international enquiries, which the business might not have targeted. The business should have proper plans to address such opportunities.

2.2.6.3 *Concerns:*

2.2.6.3.1 There are a number of obstacles, which an e-commerce venture needs to overcome. Trust of customers in a web venture is an important concern. Many customers hesitate to deal with a web venture as they are not sure of the type of products and services they will receive. This is particularly true in a B2C venture like e-shop, e-mall or e-auction site. Traditional business with well established brands and goodwill and having a physical presence face less resistance from customers in this regard than a pure e-venture.

2.2.6.3.2 Many B2C ventures have ultimately to deliver a product or service in physical form to the customer for a deal contracted through Internet. This needs proper logistics, an efficient distribution network, and control over quality of product or service delivered. These issues are not technology related and any let off in this area can drive the customer away to the competitor or from e-commerce.

2.2.6.3.3 The privacy of information on the customer's preferences, credit card and bank account details etc. and customers' faith in a system where such privacy is stated to be ensured are important issues to be addressed. These are mainly technological issues, but human factor is important both at the business and at the customers' end and also in building the trust in the system.

2.2.6.3.4 Security of a transaction, authenticity of a deal, identification of a customer etc. are important technological and systems issues, which are major sources of concern to e-commerce. Equally important are questions of repudiation of a deal, applicability of law, jurisdiction of tax laws etc. These are important to all forms of e-commerce, whether B2C or B2B and all segments of business, i.e, manufacturing, services and finance and are addressed in different chapters of this report.

2.2.6.3.5 Accessibility to Internet by the consumers is an important issue in B2C domain. This is particularly so in countries like India where penetration of PCs and other devices to households for access to Internet is minimal. Also important are availability of bandwidth and other infrastructure for faster and easier access. Considering that e-commerce aims at global market, deficiencies of these kinds in the developing world are no longer concerns confined to these areas, but are global e-commerce concerns.

2.2.7 *Business to Business (B2B)*

2.2.7.1 As opposed to B2C e-commerce, in B2B domain, the parties to a deal are at different points of the product supply chain. Typically, in a B2B type domain, a company, its suppliers, dealers and bankers to all the parties are networked to finalize and settle all aspects of a deal, online. Perhaps, only the goods in different stages of processing physically move from the supplier to the dealer. This scenario can be extended to include the shipper, providers of different ancillary services, IT service provider and the payment system gateway, etc., depending on the degree of sophistication of the available systems.

2.2.7.2 Another important feature of a B2B domain, as distinct from B2C, is that business information / data is integrated to the back office systems of parties to a deal and the state of straight through processing (STP) or near STP is achieved. This is a very significant aspect of B2B model of e-commerce, which results in improved profits through lowering cost and reducing inventories.

2.2.7.3 For example, in a B2B environment, typically, the back office system of a company controls inventory requirement with reference to the order book position updated regularly on the basis of orders received from dealers through Internet. At the optimum level of inventory it raises a purchase order with the supplier, whose system in turn, processes the order and confirms supply. Buyer company's system issues debit instructions on its bank account for payment to the supplier. The buyer's bank credits seller's bank with the cost of sale though a payment gateway or through RTGS system. Similar series of transaction processes are also initiated between the company and its dealers and their respective banks. Once e-commerce relationship is established between the firms, the transactions of the type shown above can be processed with minimal human intervention and on 24 hours a day and 7 day a week basis.

2.2.7.4 New business models are emerging in B2B domain. There are portals which offer a meeting ground to buyers and sellers of different products in supply chain, more like a buyer-seller meet in international business. This has enabled relatively smaller companies to enter the global market. Banks in the portal offer financial services for deals settled through the portal.

2.2.7.5 Technology and networking are important constituents of a B2B type of business domain. Earlier, only large firms could have access to such technology and they used private networks with interface to each other for information flow and transaction processing. A major concern used to be compatibility of EDI platforms across different B2B partners. Internet with WWW and other standard technology have offered opportunity to relatively smaller and medium sized firms to integrate their operations in B2B model and take advantage of the benefits it offers. It has also led to standardization of software platforms.

2.2.7.6 Other new forms of business models in B2B domain are Application Service Providers (ASP) and Service Integrators. ASPs offer application software online to e-commerce companies who pay for the same according to the use without owning it. Often entire back office processing is taken care of by ASPs and other service integrators. However, the utility of such service providers will to a large extent depend on the business strategy of the e-venture.

2.2.7.7 The concerns of B2B e-commerce are similar to those of B2C, discussed earlier. The security issues are more pronounced because of high value transfers taking place through the net. So also are the issues relating to privacy of information, law, tax repudiation etc. The other issues of importance to a B2B firm are the choice of appropriate technology, the issue of build or outsource, maintenance and training of personnel, etc., since they involve large investments and are critical to success.

2.2.7.8 Several studies have attempted to assess the relative importance of B2B and B2C business domains. There is wide difference in estimates of volume of business transacted over Internet and its components under B2C and B2B. However, most studies agree that volume of transactions in B2B domain far exceeds that in B2C. This is expected result. There is also a growing opinion that the future of e-business lies in B2B domain, as compared to B2C. This has several reasons some of which are already discussed earlier, like low penetration of PCs to households, low bandwidth availability etc., in a large part of the world. The success of B2C ventures depends to a large extent on the shopping habits of people in different parts of the world. A survey sponsored jointly by Confederation of Indian Industries and Infrastructure Leasing and Financial Services on e-commerce in India in 1999 made the following observations. 62% of PC owners and 75% of PC non-owners but who have access to Internet would not buy through the net, as they were not sure of the product offered. The same study estimated the size of B2B business in India by the year 2001 to be varying between Rs. 250 billion to Rs. 500 billion. In a recent study done by Arthur Anderson, it has been estimated that 84% of total e-business revenue is generated from B2B segment and the growth prospects in this segment are substantial. It has estimated the revenues to be anywhere between US $ 2.7 trillion to over US $ 7 trillion within the next three years (2003).

2.3 *The Growth of Internet Banking and common products:*

2.3.1 Internet Banking (Fig. 1) is a product of e-commerce in the field of banking and financial services. In what can be described as B2C domain for banking industry, Internet Banking offers different online services like balance enquiry, requests for cheque books, recording stop-payment instructions, balance transfer instructions, account opening and other forms of traditional banking services. Mostly, these are traditional services offered through Internet as a new delivery channel. Banks are also offering payment services on behalf of their customers who shop in different e-shops, e-malls etc. Further, different banks have different levels of such services offered, starting from level-1 where only information is disseminated through Internet to level-3 where online transactions are put through. These aspects have been dealt with in brief in the introductory chapter and again detailed products and services are discussed in chapters 3 and 4. Hence, in the following paragraphs I-banking concerns in B2B domain are discussed.

2.3.2 Considering the volume of business e-commerce, particularly in B2B domain, has been generating, it is natural that banking would position itself in an intermediary role in settling the transactions and offering other trade related services. This is true both in respect of B2C and B2B domains. Besides, the traditional role of financial intermediary and settlement agents, banks have also exploited new opportunities offered by Internet in the fields of integrated service providers, payment gateway services, etc. However, the process is still evolving and banks are repositioning themselves based on new emerging e-commerce business models.

2.3.3 In B2B scenario, a new form of e-commerce market place is emerging where various players in the production and distribution chain are positioning themselves and are achieving a kind of integration in business information flow and processing (STP or near STP) leading to efficiencies in the entire supply chain and across industries. Banks are positioning themselves in such a market in order to be a part of the financial settlements arising out of transactions of this market and providing wholesale financial services. This needs integration of business information flow not only across the players in the supply chain, but with the banks as well.

2.3.4 With the integration of business information flow and higher degree of transparency, the banks and other financial services institutions have lost some of the information advantage they used to enjoy and factor in to pricing of their products. However, such institutions have the advantage of long standing relationships, goodwill and brand, which are important sources of assurance in a virtual market. Banks are in fact, converting this goodwill into a business component in e-commerce scenario in providing settlement and other financial services. Some banks have also moved to providing digital certificates for transactions through e-markets.

2.3.5 Banks' strategies in B2B market are responses to different business models emerging in e-commerce. A recent study by Arthur Andersen shows that banks and financial service institutions generally adopt one of three business models to respond to e-business challenges. In the first place, they treat it as an extension of existing business without any significant changes other than procedural and what technology demands. The second strategy takes the same approach as the first but introduces structural changes to the underlying business. In the third approach banks launch e-business platform as a different business from the existing core business and as a different brand of product. There is no definite answer as to which approach is appropriate. Perhaps it depends on the type of market the bank is operating, its existing competencies and the legal and regulatory environment. It is, however, sure that e-banking is evolving beyond the traditional limits of banking and many new products / services are likely to emerge as e-commerce matures.

Chapter-3 - International experience

3.1 Internet banking has presented regulators and supervisors worldwide with new challenges. The Internet, by its very nature, reaches across borders and is, for this reason, engaging the attention of regulatory and supervisory authorities all over the world. The experience of various countries, as far as Internet banking is concerned, is outlined in this chapter.

3.2 U.S.A.

3.2.1 In the USA, the number of thrift institutions and commercial banks with transactional web-sites is 1275 or 12% of all banks and thrifts. Approximately 78% of all commercial banks with more than $5 billion in assets, 43% of banks with $500 million to $5 billion in assets, and 10% of banks under $ 500 million in assets have transactional web-sites. Of the 1275-thrifts/commercial banks offering transactional Internet banking, 7 could be considered 'virtual banks'. 10 traditional banks have established Internet branches or divisions that operate under a unique brand name. Several new business process and technological advances such as Electronic Bill Presentment and Payment (EBPP), handheld access devices such as Personal Digital Assistants (PDAs), Internet Telephone and Wireless Communication channels and phones are emerging in the US market. A few banks have become Internet Service Providers (ISPs), and banks may become Internet portal sites and online service providers in the near future. Reliance on third party vendors is a common feature of electronic banking ventures of all sizes and degrees of sophistication in the US. Currently, payments made over the Internet are almost exclusively conducted through existing payment instruments and networks. For retail e-commerce in the US, most payments made over the Internet are currently completed with credit cards and are cleared and settled through existing credit card clearing and settlement systems. Efforts are under way to make it easier to use debit cards, cheques and the Automated Clearing House (ACH) to make payments over the Internet. Versions of e-money, smart cards, e-cheques and other innovations are being experimented with to support retail payments over the Internet.

3.2.2 There is a matrix of legislation and regulations within the US 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. Federal and state laws, regulations, and court decisions, and self-regulation among industries groups provide the legal and operational framework for Internet commerce and banking in the USA. The international model laws promulgated by the United Nations Commission on International Trade Law (UNCITRAL) provide the guidance to the member nations on the necessity for revising existing legal structures to accommodate electronic transactions. Some important laws of general application to commercial activity over the Internet within the US are the Uniform Commercial Code (UCC), the Uniform Electronic Transaction Act (UETA) (which provides that electronic documents and contracts should not be disqualified as legal documents particularly because of their electronic form), various state laws and regulations on digital signatures and national encryption standards and export regulations. Many states already have digital signature and other legislation to enable e-commerce. State laws in this area differ but the trend is towards creating legislation, which is technology neutral. The E-sign Act, a new US law that took effect on October 1, 2000, validates contracts concluded by electronic signatures and equates them to those signed with ink on paper. Under the Act, electronic signatures using touch-tones (on a telephone), retinal scans and voice recognition are also acceptable ways of entering into agreements. The E-sign Act takes a technological neutral approach and does not favor the use of any particular technology to validate an electronic document. The Act however does not address issues relating to which US state's laws would govern an online transaction and which state's code would have jurisdiction over a dispute.

3.2.3 The Gramm - Leach – Bliley (GLB) Act has substantially eased restrictions on the ability of banks to provide other financial services. It has established new rules for the protection of consumer financial information. The Inter-agency Statement on Electronic Financial Services and Consumer Compliance (July 1998) addresses consumer protection laws and describe how they can be met in the context of electronic delivery. In addition, the Federal Reserve Board has issued a request for comment on revised proposals that would permit electronic delivery of federally mandated disclosures under the five consumer protection regulations of the FRB (Regulations B, DD, E, M & Z).

3.2.4 The Interpretive Ruling of the Office of the Comptroller of Currency (OCC) authorizes a national bank to 'perform, provide or deliver through electronic means and facilities any activity, functions, product or service that it is otherwise authorized to perform, provide or deliver'. 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, the safety and soundness of the bank, and the protection of the banks' customers. Currently, all banks, whether they are 'Internet only' or traditional banks must apply for a charter according to existing guidelines. The five federal agencies - Federal Deposit Insurance Corporation (FDIC), Federal Reserve System (FRS), Office of the Comptroller of Currency (OCC), Office of Thrift Supervision (OTS) and the National Credit Union Association (NCUA) supervise more than 20,000 institutions. In addition, each state has a supervisory agency for the banks that it charters. Most financial institutions in the US face no prerequisite conditions or notification requirements for an existing banking institution to begin electronic banking activities. For these banks, supervisors gather information on electronic banking during routine annual examination. Newly chartered Internet banks are subject to the standard chartering procedures. For thrift institutions, however, OTS has instituted a 30-day advance notification requirement for thrift institutions that plan to establish a transactional web site. A few State banking departments have instituted a similar notification requirement for transactional Internet banking web sites.

3.2.5 Supervisory policy, licensing, legal requirements and consumer protection are generally similar for electronic banking and traditional banking activities. Internet banks are also subject to the same rules, regulations and policy statement as traditional banks. However, in response to the risks posed by electronic banking, federal banking agencies have begun to issue supervisory guidelines and examination procedures for examiners who review and inspect electronic banking applications. Although specialized banking procedures are used in some areas of Internet banking activities, the existing information technology examination framework that addresses access controls, information security, business recovery and other risk areas generally continues to be applicable. To assist supervisors in monitoring the expansion of Internet banking, state chartered and national banks have been required since June 1999 to report their websites' 'Uniform Resource Locators' (URL) in the Quarterly Reports of Financial Condition that are submitted to supervisors. In addition, examiners review the potential for reputational risk associated with web-site information or activities, the potential impact of various Internet strategies on an institution's financial condition, and the need to monitor and manage outsourcing relationships. To address these risks, the OCC is developing specific guidance for establishing 'Internet only' banks within the US. The Banking Industry Technology Secretariat recently announced the formation of a security lab to test and validate the security of software and hardware used by banking organizations. If a bank is relying on a third party provider, it is accepted that it should be able to understand the provided information security programme to effectively evaluate the security system's ability to protect bank and customer data. Examination of service providers' operations, where necessary, is conducted by one or more Federal banking agencies pursuant to the Bank Services Company Act, solely to support supervision of banking organizations.

3.2.6 The Federal Financial Institutions Examination Council (FFIEC) introduced the Information Systems (IS) rating system to be used by federal and state regulators to assess uniformly financial and service provider risks introduced by information technology and to identify those institutions and service providers requiring special supervisor attention. The FFIEC has recently renamed the system as Uniform Rating System for IT (URSIT), which has enhanced the audit function. The importance of risk management procedure has been reinforced under the revised system.

3.2.7 Some characteristics of e-money products such as their relative lack of physical bulk, their potential anonymity and the possibility of effecting fast and remote transfers make them more susceptible than traditional systems to money laundering activities. The OCC guidelines lay down an effective 'know your customer' policy. Federal financial institutions, regulators, Society for Worldwide Interbank Financial Telecommunications (SWIFT) and Clearing House Interbank Payment System (CHIPS) have issued statements encouraging participants to include information on originators and beneficiaries.

3.3 U.K.

3.3.1 Most banks in U.K. are offering transactional services through a wider range of channels including Wireless Application Protocol (WAP), mobile phone and T.V. A number of non-banks have approached the Financial Services Authority (FSA) about charters for virtual banks or 'clicks and mortar' operations. There is a move towards banks establishing portals.

3.3.2 The Financial Services Authority (FSA) is neutral on regulations of electronic banks. The current legislation, viz. the Banking Act 1987 and the Building Societies Act, provides it with the necessary powers and the current range of supervisory tools. A new legislation, the Financial Services and Market Bill, offers a significant addition in the form of an objective requiring the FSA to promote public understanding of the financial system. There is, therefore, no special regime for electronic banks. A draft Electronic Banking Guidance for supervisors has, however, been developed. A guide to Bank Policy has also been published by the FSA which is technology neutral, but specifically covers outsourcing and fraud. The FSA also maintains bilateral discussions with other national supervisors and monitors developments in the European Union (EU) including discussions by the Banking Advisory Committee and Group de Contract. New legislation on money laundering has been proposed and both the British Bankers Association and the FSA have issued guidance papers in this regard.

3.3.3 The FSA is actively involved in the Basle Committee e-banking group which has identified authorization, prudential standards, transparency, privacy, money laundering and cross border provision as issues where there is need for further work. The FSA has also been supporting the efforts of the G7 Financial Stability Forum, which is exploring common standards for financial market, which is particularly relevant to the Internet, which reaches across all borders.

3.3.4 The Financial Services and Markets Bill will replace current powers under the 1987 Banking Act giving the FSA statutory authority for consumer protection and promotion of consumer awareness. Consumer compliance is required to be ensured via desk based and on site supervision. The FSA has an Authorization and Enforcement Division, which sees if web sites referred to them are in violation of U.K. laws.

3.3.5 The FSA has issued guidelines on advertising in U.K. by banks for deposits, investments and other securities, which apply to Internet banking also. The guidelines include an Appendix on Internet banking. The FSA's supervisory policy and powers in relation to breaches in the advertising code (viz. invitation by any authorized person to take a deposit within U.K., fraudulent inducements to make a deposit, illegal use of banking names and descriptions, etc.) are the same for Internet banking as they are for conventional banking. The FSA does not regard a bank authorized overseas, which is targeting potential depositors in its home market or in third countries as falling within U.K. regulatory requirements solely by reason of its web site being accessible to Internet users within the U.K., as the advertisements are not aimed at potential U.K. depositors.

3.4 Scandinavia

3.4.1 Swedish and Finnish markets lead the world in terms of Internet penetration and the range and quality of their online services. Merita Nordbanken (MRB) (now Nordic Bank Holding, a merger between Finland's Merita and Nordbanker of Sweden) leads in "log-ins per month" with 1.2 million Internet customers, and its penetration rate in Finland (around 45%) is among the highest in the world for a bank of 'brick and mortar' origin. Standinaviska Easkilda Banken (SEB) was Sweden's first Internet bank, having gone on-line in December 1996. It has 1,000 corporate clients for its Trading Station – an Internet based trading mechanism for forex dealing, stock-index futures and Swedish treasury bills and government bonds. Swedbank, is another large-sized Internet bank. Almost all of the approximately 150 banks operating in Norway had established "net banks". In Denmark, the Internet banking service of Den Danske offers funds transfers, bill payments, etc.

3.4.2 The basic on-line activity is paying bills. Swedbank was the first bank in the world to introduce Electronic Bill Presentment and Payment (EBPP) and now handles 2 million bill payment a month. E-shopping is another major Internet banking service. MNB has an on-line "mall" of, more than 900 shops, which accepts its "Solo" payment system. Swedbank has a similar system called "Direct". Besides using advanced encryption technology, the Scandenavian banks have adopted a basic but effective system known as "challenge response logic", which involves a list of code numbers sent to every online client and used in sequence, in combination with their password or PIN. This gives each transaction a unique code, and has so far proved safe. Some banks use even more sophisticated versions of the same technique. It is not a common practice to use third party vendors for services.

3.4.3 In Sweden, no formal guidance has been given to examiners by the Sverigesbank on e-banking. General guidelines apply equally to Internet banking activities. Contractual regularization between customers and the bank is a concern for regulators and is being looked into by the authorities.

3.4.4 The role of the Bank of Finland (Suomen Parkki) has been, as part of general oversight of financial markets in Finland, mainly to monitor the ongoing development of Internet banking without active participation. Numerous issues concerning Internet banking have, however, been examined by the Bank of Finland.

3.4.5 All Internet banking operating from a Norwegian platform are subject to all regular banking regulations, just as any other bank. As part of the standard regulation, there is also a specific regulation on the banks' use of IT. This regulation dates from 1992 when Internet banking was not the main issue, but it covers all IT systems, including Internet banking. The regulation secures that banks' purchase, development, use and phase out of IT systems is conducted in a safe and controlled manner. An Act relating to Payment systems defines payment systems as those which are based on standardized terms for transfer of funds from or between customer accounts in banks/financial undertakings when the transfer is based on use of payment cards, numeric codes or any other form of independent user identification. Internet banking is covered by this regulation. The Banking, Insurance and Securities Commission may order for implementation of measures to remedy the situation if there is a violation of provisions.

3.4.6 In addition to their national laws, countries in Europe are also expected to implement European Union (EU) directives. In 1995, the EU passed a Europe-wide Data Protection Directive aimed at granting individuals greater protection from abuses of their personal information. It also passed the Telecommunications Directive that prescribes special protection in relation to telephones, digital TVs, mobile communications, etc. Every EU country is to have a privacy commissioner to enforce the regulations as they apply within the EU. The EU directive on electronic signature is also required to be implemented in national laws.

3.5 Other Countries

3.5.1 *Australia:*

3.5.1.1 Internet Banking in Australia is offered in two forms: web-based and through the provision of proprietary software. Initial web-based products have focused on personal banking whereas the provision of proprietary software has been targeted at the business/corporate sector. Most Australian-owned banks and some foreign subsidiaries of banks have transactional or interactive web-sites. Online banking services range from FIs' websites providing information on financial products to enabling account management and financial transactions. Customer services offered online include account monitoring (electronic statements, real-time account balances), account management (bill payments, funds transfers, applying for products on-line) and financial transactions (securities trading, foreign currency transactions). Electronic Bill Presentment and Payment (EBPP) is at an early stage. Features offered in proprietary software products (enabling business and corporation customers to connect to the financial institutions (via dial-up/leased line/extranet) include account reporting, improved reconciliation, direct payments, payroll functionality and funds transfer between accounts held at their own or other banks. Apart from closed payment systems (involving a single payment-provider), Internet banking and e-commerce transactions in Australia are conducted using long-standing payment instruments and are cleared and settled through existing clearing and settlement system. Banks rely on third party vendors or are involved with outside providers for a range of products and services including e-banking. Generally, there are no 'virtual' banks licensed to operate in Australia.

3.5.1.2 The Electronic Transactions Act, 1999 provides certainty about the legal status of electronic transactions and allows for Australians to use the Internet to provide Commonwealth Departments and agencies with documents which have the same legal status as traditional paperwork. The Australian Securities and Investments Commission (ASIC) is the Australian regulator with responsibility for consumer aspects of banking, insurance and superannuation and as such, it is responsible for developing policy on consumer protection issues relating to the Internet and e-commerce. ASIC currently has a draft proposal to expand the existing Electronic Funds Transfer Code of

Conduct (a voluntary code that deals with transactions initiated using a card and a PIN) to cover all forms of consumer technologies, including stored value cards and other new electronic payment products. Australia's anti-money laundering regulator is the Australian Transaction Reports and Analysis Centre (AUSTRAC).

3.5.1.3 Responsibility for prudential supervisory matters lies with the Australian Prudential Regulation Authority (APRA). APRA does not have any Internet specific legislation, regulations or policy, and banks are expected to comply with the established legislation and prudential standards. APRA's approach to the supervision of e-commerce activities, like the products and services themselves, is at an early stage and is still evolving. APRA's approach is to visit institutions to discuss their Internet banking initiatives. However, APRA is undertaking a survey of e-commerce activities of all regulated financial institutions. The growing reliance on third party or outside providers of e-banking is an area on which APRA is increasingly focusing.

3.5.2 *New Zealand:*

3.5.2.1 Major banks offer Internet banking service to customers, operate as a division of the bank rather than as a separate legal entity.

3.5.2.2 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 supervision regulations that apply only to Internet banking. Supervision is based on public disclosure of information rather than application of detailed prudential rules. These disclosure rules apply to Internet banking activity also.

3.5.3 *Singapore:*

3.5.3.1 The Monetary Authority of Singapore (MAS) has reviewed its current framework for licensing, and for prudential regulation and supervision of banks, to ensure its relevance in the light of developments in Internet banking, either as an additional channel or in the form of a specialized division, or as stand-alone entities (Internet Only Banks), owned either by existing banks or by new players entering the banking industry. The existing policy of MAS already allows all banks licensed in Singapore to use the Internet to provide banking services. MAS is subjecting Internet banking, including IOBs, to the same prudential standards as traditional banking. It will be granting new licences to banking groups incorporated in Singapore to set up bank subsidiaries if they wish to pursue new business models and give them flexibility to decide whether to engage in Internet banking through a subsidiary or within the bank (where no additional licence is required). MAS also will be admitting branches of foreign incorporated IOBs within the existing framework of admission of foreign banks.

3.5.3.2 As certain types of risk are accentuated in Internet banking, a risk – based supervisory approach, tailored to individual banks' circumstances and strategies, is considered more appropriate by MAS than "one-size-fits-all" regulation. MAS requires public disclosures of such undertakings, as part of its requirement for all banks and enhance disclosure of their risk management systems. It is issuing a consultative document on Internet banking security and technology risk management. In their risk management initiatives for Internet banking relating to security and technology related risks, banks should (a) implement appropriate workflow, authenticated process and control procedures surrounding physical and system access (b) develop, test, implement and maintain disaster recovery and business contingency plans (c) appoint an independent third party specialist to assess its security and operations (d) clearly communicate to customers their policies with reference to rights and responsibilities of the bank and customer, particularly issues arising from errors in security systems and related procedures. For liquidity risk, banks, especially IOBs, should establish robust liquidity contingency plans and appropriate Asset-Liability Management systems. As regards operational risk, banks should carefully manage outsourcing of operations, and maintain comprehensive audit trails of all such operations. As far as business risk is concerned, IOBs should maintain and continually update a detailed system of performance measurement.

3.5.3.3 MAS encourages financial institutions and industry associations such as the Associations of Banks in Singapore (ABS) to play a proactive role in educating consumers on benefits and risks on new financial products and services offered by banks, including Internet banking services.

3.5.4 *Hong Kong:*

3.5.4.1 There has been a spate of activity in Internet banking in Hong Kong. Two virtual banks are being planned. It is estimated that almost 15% of transactions are processed on the Internet. During the first quarter of 2000, seven banks have begun Internet services. Banks are participating in strategic alliances for e-commerce ventures and are forming alliances for Internet banking services delivered through Jetco (a bank consortium operating an ATM network in Hong Kong). A few banks have launched transactional mobile phone banking earlier for retail customers.

3.5.4.2 The Hong Kong Monetary Authority (HKMA) requires that banks must discuss their business plans and risk management measures before launching a transactional website. HKMA has the right to carry out inspections of security controls and obtain reports from the home supervisor, external auditors or experts commissioned to produce reports. HKMA is developing specific guidance on information security with the guiding principle that security should be “fit for purpose”. HKMA requires that risks in Internet banking system should be properly controlled. The onus of maintaining adequate systems of control including those in respect of Internet banking ultimately lies with the institution itself. Under the Seventh Schedule to the Banking ordinance, one of the authorization criteria is the requirement to maintain adequate accounting system and adequate systems control. Banks should continue to acquire state-of-the art technologies and to keep pace with developments in security measures. The HKMA’s supervisory approach is to hold discussions with individual institutions who wish to embark on Internet banking to allow them to demonstrate how they have properly addressed the security systems before starting to provide such services, particularly in respect of the following – (i) encryption by industry proven techniques of data accessible by outsiders, (ii) preventive measures for unauthorized access to the bank’s internal computer systems, (iii) set of comprehensive security policies and procedures, (iv) reporting to HKMA all security incidents and adequacy of security measures on a timely basis. At present, it has not been considered necessary to codify security objectives and requirements into a guideline. The general security objectives for institutions intending to offer Internet banking services should have been considered and addressed by such institutions.

3.5.4.3 HKMA has issued guidelines on ‘Authorization of Virtual Banks’ under Section 16(10) of the Banking Ordinance under which (i) the HKMA will not object to the establishment of virtual banks in Hong Kong provided they can satisfy the same prudential criteria that apply to conventional banks, (ii) a virtual bank which wishes to carry on banking business in Hong Kong must maintain a physical presence in Hong Kong; (iii) a virtual bank must maintain a level of security which is appropriate to the type of business which it intends to carry out. A copy of report on security of computer hardware, systems, procedures, controls etc. from a qualified independent expert should be provided to the HKMA at the time of application, (iv) a virtual bank must put in place appropriate policies, procedures and controls to meet the risks involved in the business; (v) the virtual bank must set out clearly in the terms and conditions for its service what are the rights and obligations of its customers (vi) Outsourcing by virtual banks to a third party service provider is allowed, provided HKMA's guidelines on outsourcing are complied with. There are principles applicable to locally incorporated virtual banks and those applicable to overseas-incorporated virtual banks.

3.5.4.4 Consumer protection laws in Hong Kong do not apply specifically to e-banking but banks are expected to ensure that their e-services comply with the relevant laws. The Code of Banking Practice is being reviewed to incorporate safeguards for customers of e-banking.

3.5.4.5 Advertising for taking deposits to a location outside Hong Kong is a violation unless disclosure requirements are met. Consideration is being given as to whether this is not too onerous in the context of the global nature of the Internet.

3.5.4.6 Recognising the relevance of Public Key Infrastructure (PKI) in Hong Kong to the development of Internet banking and other forms of e-commerce, the government of Hong Kong has invited the Hong Kong Postal Authority to serve as public Certificate Authority (CA) and to establish the necessary PKI infrastructure. There is no bar, however, on the private sector setting up CAs to serve the specific needs of individual networks. There should be cross-references and mutual recognition of digital signatures among CAs. The Government is also considering whether and, if so, how the legal framework should be strengthened to provide firm legal basis for electronic transactions (particularly for digital signatures to ensure non-repudiation of electronic messages and transactions).

3.5.5 *Japan:*

3.5.5.1 Banks in Japan are increasingly focusing on e-banking transactions with customers.

Internet banking is an important part of their strategy. While some banks provide services such as inquiry, settlement, purchase of financial products and loan application, others are looking at setting up finance portals with non-finance business corporations. Most banks use outside vendors in addition to in-house services.

3.5.5.2 The current regulations of the Bank of Japan on physical presence of bank branches are undergoing modifications to take care of licensing of banks and their branches with no physical presence. The Report of the Electronic Financial Services Study Group (EFSSG) has made recommendations regarding the supervision and regulation of electronic financial services. Financial institutions are required to take sufficient measures for risk management of service providers and the authorities are required to verify that such measures have been taken. Providing information about non-financial businesses on a bank web site is not a violation as long as it does not constitute a business itself.

3.5.5.3 With respect to consumer protection it is felt that guidance and not regulations should encourage voluntary efforts of individual institutions in this area. Protection of private information, however, is becoming a burning issue in Japan both within and outside the field of e-banking. Japanese banks are currently requested to place disclosure publications in their offices (branches) by the law. However, 'Internet Only banks' are finding it difficult to satisfy this requirement. The Report of the EFSSG recommends that financial service providers that operate transactional website should practice online disclosure through electronic means at the same timing and of equivalent contents as paper based disclosure. They should also explain the risks and give customers a fair chance to ask queries. The Government of Japan intends to introduce comprehensive Data Protection Legislation in the near future. .

3.5.5.4 There are no restrictions or requirements on the use of cryptography. The Ministry of International Trade and Industry (MITI)'s approval is required to report encryption technology.

3.6 Conclusion

World over, electronic banking is making rapid strides due to evolving communication technology. Penetration of Internet banking is increasing in most countries. Wireless Application Protocol (WAP) is an emerging service which banks worldwide are also offering. The stiff competition in this area exposes banks to substantial risks. The need is being felt overseas that transparency and disclosure requirements should be met by the e-banking community. While existing regulations and legislations applicable to traditional banking are being extended to banks' Internet banking and electronic banking services, it is recognized that Internet security, customer authentication and other issues such as technology outsourcing pose unique risks. Central Banks worldwide are addressing such issues with focused attention. Special legislations and regulations are being framed by the regulators and supervisors for proper management of the different types of risks posed by these services. The reliance on outsourcing is an area where overseas regulators and supervisors are focusing their attention, with banks having to regularly review and test business continuity, recovery and incidence response plans in order to maintain their reputation of trust. Consumer protection and data privacy are areas which assume great significance when banking transactions are carried over a medium as insecure as the Internet. Many countries are looking at special consumer protection/data privacy legislation for an e-commerce environment. The presence of 'virtual banks' or 'Internet only banks' and the licensing requirements required for such entities are also areas which are being looked into by overseas authorities. There has also been co-operation among the regulators and supervisors to meet the challenges of 'virtual' cross border e-banking, particularly in the light of the possibility of increased money laundering activities through the medium of Internet. Internet banking is universally seen as a welcome development, and efforts are being made to put in place systems to manage and control the risks involved without restricting this service.

Chapter -4 -The Indian Scenario

4.1 The entry of Indian banks into Net Banking

4.1.1 Internet banking, both as a medium of delivery of banking services and as a strategic tool for business development, has gained wide acceptance internationally and is fast catching up in India with more and more banks entering the fray. India can be said to be on the threshold of a major banking revolution with net banking having already been unveiled. A recent questionnaire to which 46 banks responded, has revealed that at present, 11 banks in India are providing Internet banking services at different levels, 22 banks propose to offer Internet banking in near future while the remaining 13 banks have no immediate plans to offer such facility.

4.1.2 At present, the total Internet users in the country are estimated at 9 lakh. However, this is expected to grow exponentially to 90 lakh by 2003. Only about 1% of Internet users did banking online in 1998. This increased to 16.7% in March 2000.* The growth potential is, therefore, immense. Further incentives provided by banks would dissuade customers from visiting physical branches, and thus get 'hooked' to the convenience of arm-chair banking. The facility of accessing their accounts from anywhere in the world by using a home computer with Internet connection, is particularly fascinating to Non-Resident Indians and High Networth Individuals having multiple bank accounts.

4.1.3 Costs of banking service through the Internet form a fraction of costs through conventional methods. Rough estimates assume teller cost at Re.1 per transaction, ATM transaction cost at 45 paise, phone banking at 35 paise, debit cards at 20 paise and Internet banking at 10 paise per transaction. The cost-conscious banks in the country have therefore actively considered use of the Internet as a channel for providing services. Fully computerized banks, with better management of their customer base are in a stronger position to cross-sell their products through this channel.

* Source : India Research May 29 , 2000 , Kotak Securities

4.2 Products and services offered

4.2.1 Banks in India are at different stages of the web-enabled banking cycle. Initially, a bank, which is not having a web site, allows its customer to communicate with it through an e-mail address; communication is limited to a small number of branches and offices which have access to this e-mail account. As yet, many scheduled commercial banks in India are still in the first stage of Internet banking operations.

4.2.2 With gradual adoption of Information Technology, the bank puts up a web-site that provides general information on the banks, its location, services available e.g. loan and deposits products, application forms for downloading and e-mail option for enquiries and feedback. It is largely a marketing or advertising tool. For example, Vijaya Bank provides information on its web-site about its NRI and other services. Customers are required to fill in applications on the Net and can later receive loans or other products requested for at their local branch. A few banks provide the customer to enquire into his demat account (securities/shares) holding details, transaction details and status of instructions given by him. These web sites still do not allow online transactions for their customers.

4.2.3 Some of the banks permit customers to interact with them and transact electronically with them. Such services include request for opening of accounts, requisition for cheque books, stop payment of cheques, viewing and printing statements of accounts, movement of funds between accounts within the same bank, querying on status of requests, instructions for opening of Letters of Credit and Bank Guarantees etc. These services are being initiated by banks like ICICI Bank Ltd., HDFC Bank Ltd. Citibank, Global Trust Bank Ltd., UTI Bank Ltd., Bank of Madura Ltd., Federal Bank Ltd. etc. Recent entrants in Internet banking are Allahabad Bank (for its corporate customers through its ‘Allnet’ service) and Bank of Punjab Ltd. State Bank of India has announced that it will be providing such services soon. Certain banks like ICICI Bank Ltd., have gone a step further within the transactional stage of Internet banking by allowing transfer of funds by an account holder to any other account holder of the bank.

4.2.4 Some of the more aggressive players in this area such as ICICI Bank Ltd., HDFC Bank Ltd., UTI Bank Ltd., Citibank, Global Trust Bank Ltd. and Bank of Punjab Ltd. offer the facility of receipt, review and payment of bills on-line. These banks have tied up with a number of utility companies. The ‘Infinity’ service of ICICI Bank Ltd. also allows online real time shopping mall payments to be made by customers. HDFC Bank Ltd. has made e-shopping online and real time with the launch of its payment gateway. It has tied up with a number of portals to offer business-to-consumer (B2C) e-commerce transactions. The first online real time e-commerce credit card transaction in the country was carried out on the Easy3shoppe.com shopping mall, enabled by HDFC Bank Ltd. on a VISA card.

4.2.5 Banks like ICICI Bank Ltd., HDFC Bank Ltd. etc. are thus looking to position themselves as one stop financial shops. These banks have tied up with computer training companies, computer manufacturers, Internet Services Providers and portals for expanding their Net banking services, and widening their customer base. ICICI Bank Ltd. has set up a web based joint venture for on-line distribution of its retail banking products and services on the Internet, in collaboration with Satyam Infoway, a private ISP through a portal named as icicisify.com. The customer base of www.satyamonline.com portal is also available to the bank. Setting up of Internet kiosks and permeation through the cable television route to widen customer base are other priority areas in the agendas of the more aggressive players. Centurion Bank Ltd. has taken up equity stake in the teauction.com portal, which aims to bring together buyers, sellers, registered brokers, suppliers and associations in the tea market and substitute their physical presence at the auctions announced.

4.2.6 Banks providing Internet banking services have been entering into agreements with their customers setting out the terms and conditions of the services. The terms and conditions include information on the access through user-id and secret password, minimum balance and charges, authority to the bank for carrying out transactions performed through the service, liability of the user and the bank, disclosure of personal information for statistical analysis and credit scoring also, non-transferability of the facility, notices and termination, etc.

4.2.7 The race for market supremacy is compelling banks in India to adopt the latest technology on the Internet in a bid to capture new markets and customers. HDFC Bank Ltd. with its ‘Freedom- the e-Age Saving Account’ Service, Citibank with ‘Suvidha’ and ICICI Bank Ltd. with its ‘Mobile Commerce’ service have tied up with cellphone operators to offer Mobile Banking to their customers. Global Trust Bank

Ltd. has also announced that it has tied up with cellular operators to launch mobile banking services. Under Mobile Banking services, customers can scan their accounts to seek balance and payments status or instruct banks to issue cheques, pay bills or deliver statements of accounts. It is estimated that by 2003, cellular phones will have become the premier Internet access device, outselling personal computers. Mobile banking will further minimise the need to visit a bank branch.

4.3 The Future Scenario

4.3.1 Compared to banks abroad, Indian banks offering online services still have a long way to go. For online banking to reach a critical mass, there has to be sufficient number of users and the sufficient infrastructure in place. The 'Infinity' product of ICICI Bank Ltd. gets only about 30,000 hits per month, with around 3,000 transactions taking place on the Net per month through this service. Though various security options like line encryption, branch connection encryption, firewalls, digital certificates, automatic sign-offs, random pop-ups and disaster recovery sites are in place or are being looked at, there is as yet no Certification Authority in India offering Public Key Infrastructure which is absolutely necessary for online banking. The customer can only be assured of a secured conduit for its online activities if an authority certifying digital signatures is in place. The communication bandwidth available today in India is also not enough to meet the needs of high priority services like online banking and trading. Banks offering online facilities need to have an effective disaster recovery plan along with comprehensive risk management measures. Banks offering online facilities also need to calculate their downtime losses, because even a few minutes of downtime in a week could mean substantial losses. Some banks even today do not have uninterrupted power supply unit or systems to take care of prolonged power breakdown. Proper encryption of data and effective use of passwords are also matters that leave a lot to be desired. Systems and processes have to be put in place to ensure that errors do not take place.

4.3.2 Users of Internet Banking Services are required to fill up the application forms online and send a copy of the same by mail or fax to the bank. A contractual agreement is entered into by the customer with the bank for using the Internet banking services. In this way, personal data in the applications forms is being held by the bank providing the service. The contract details are often one-sided, with the bank having the absolute discretion to amend or supplement any of the terms at any time. For these reasons domestic customers for whom other access points such as ATMs, telebanking, personal contact, etc. are available, are often hesitant to use the Internet banking services offered by Indian banks. Internet Banking, as an additional delivery channel, may, therefore, be attractive / appealing as a value added service to domestic customers. Non-resident Indians for whom it is expensive and time consuming to access their bank accounts maintained in India find net banking very convenient and useful.

4.3.3 The Internet is in the public domain whereby geographical boundaries are eliminated. Cyber crimes are therefore difficult to be identified and controlled. In order to promote Internet banking services, it is necessary that the proper legal infrastructure is in place. Government has introduced the Information Technology Bill, which has already been notified in October 2000. Section 72 of the Information Technology Act, 2000 casts an obligation of confidentiality against disclosure of any electronic record, register, correspondence and information, except for certain purposes and violation of this provision is a criminal offence. Notification for appointment of Authorities to certify digital signatures, ensuring confidentiality of data, is likely to be issued in the coming months. Comprehensive enactments like the Electronic Funds Transfer Act in U.K. and data protection rules and regulations in the developed countries are in place abroad to prevent unauthorized access to data, malafide or otherwise, and to protect the individual’s rights of privacy. The legal issues are, however, being debated in our country and it is expected that some headway will be made in this respect in the near future.

4.3.4 Notwithstanding the above drawbacks, certain developments taking place at present, and expected to take place in the near future, would create a conducive environment for online banking to flourish. For example, Internet usage is expected to grow with cheaper bandwidth cost. The Department of Telecommunications (DoT) is moving fast to make available additional bandwidth, with the result that Internet access will become much faster in the future. This is expected to give a fillip to Internet banking in India.

4.3.5 The proposed setting up of a Credit Information Bureau for collecting and sharing credit information on borrowers of lending institutions online would give a fillip to electronic banking. The deadline set by the Chief Vigilance Commissioner for computerisation of not less than 70 percent of the bank's business by end of January 2001 has also given a greater thrust to development of banking technology. The recommendations of the Vasudevan Committee on Technological Upgradation of Banks in India have also been circulated to banks for implementation. In this background, banks are moving in for technological upgradation on a large scale. Internet banking is expected to get a boost from such developments.

4.3.6 Reserve Bank of India has taken the initiative for facilitating real time funds transfer through the Real Time Gross Settlement (RTGS) System. Under the RTGS system, transmission, processing and settlements of the instructions will be done on a continuous basis. Gross settlement in a real time mode eliminates credit and liquidity risks. Any member of the system will be able to access it through only one specified gateway in order to ensure rigorous access control measures at the user level. The system will have various levels of security, viz., Access security, 128 bit cryptography, firewall, certification etc. Further, Generic Architecture (**see fig. 2**), both domestic and cross border, aimed at providing inter-connectivity across banks has been accepted for implementation by RBI. Following a reference made this year, in the Monetary and Credit Policy statement of the Governor, banks have been advised to develop domestic generic model in their computerization plans to ensure seamless integration. The abovementioned efforts would enable online banking to become more secure and efficient.

4.3.7 With the process of dematerialisation of shares having gained considerable ground in recent years, banks have assumed the role of depository participants. In addition to customers’ deposit accounts, they also maintain demat accounts of their clients. Online trading in equities is being allowed by SEBI. This is another area which banks are keen to get into. HDFC Bank Ltd., has tied up with about 25 equity brokerages for enabling third party transfer of funds and securities through its business-to-business (B2B) portal, ‘e-Net’. Demat account holders with the bank can receive securities directly from the brokers’ accounts. The bank has extended its web interface to the software vendors of National Stock Exchange through a tie-up with NSE.IT – the infotech arm of the exchange. The bank functions as the payment bank for enabling funds transfer from its customers' account to brokers' accounts. The bank is also setting up a net broking arm, HDFC Securities, for enabling trading in stocks through the web. The focus on capital market operations through the web is based on the bank's strategy on tapping customers interested in trading in equities through the Internet. Internet banking thus promises to become a popular delivery channel not only for retail banking products but also for online securities trading.

4.3.8 An upcoming payment gateway is being developed by ICICI and Global Tele System, which will enable customers to transfer funds to banks which are part of the project. Transfer of funds can be made through credit/debit/ smart cards and cheques, with the central payment switch enabling the transactions. Banks are showing interest in this new concept, which will facilitate inter-bank funds transfers and other e-commerce transactions, thus highlighting the role of banks in e-commerce as intermediaries between buyers and sellers in the whole payment process.

4.3.9 WAP (Wireless Application Protocol) telephony is the merger of mobile telephony with the Internet. It offers two-way connectivity, unlike Mobile Banking where the customer communicates to a mailbox answering machine. Users may surf their accounts, download items and transact a wider range of options through the cellphone screen. WAP may provide the infrastructure for P2P (person to person) or P2M (person to merchant) payments. It would be ideal for transactions that do not need any cash backup, such as online investments. Use of this cutting edge technology could well determine which bank obtains the largest market share in electronic banking. IDBI Bank Ltd. has recently launched its WAP- based mobile phone banking services (offering facilities such as banking enquiry, cheque book request, statements request, details of the bank's products etc).

4.3.10 At present, there are only 2.6 phone connections per 100 Indians, against the world average of 15 connections per 100. The bandwidth capacity available in the country is only 3.2 gigabits per second, which is around 60% of current demand. Demand for bandwidth is growing by 350% a year in India. With the help of the latest technology, Indian networks will be able to handle 40 gigabits of Net traffic per second (as compared to 10 gigabits per second in Malaysia). Companies like Reliance, Bharti Telecom and the Tata Group are investing billions of rupees to build fibre optic lines and telecom infrastructure for data, voice and Internet telephony. The online population has increased from just 500,000 in 1998 to 5 million in 2000. By 2015, the online population is expected to reach 70 million. IT services is a $1.5 billion industry in India growing at a rate of 55% per annum. Keeping in view all the above developments, Internet banking is likely to grow at a rapid pace and most banks will enter into this area soon. Rapid strides are already being made in banking technology in India and Internet banking is a manifestation of this. Every day sees new tie-ups, innovations and strategies being announced by banks. State Bank of India has recently announced its intention to form an IT subsidiary. A sea change in banking services is on the cards. It would, however, be essential to have in place a proper regulatory, supervisory and legal framework, particularly as regards security of transactions over the Net, for regulators and customers alike to be comfortable with this form of banking.

Chapter- 5- Types of risks associated with Internet banking

5.1 A major driving force behind the rapid spread of i-banking all over the world is its acceptance as an extremely cost effective delivery channel of banking services as compared to other existing channels. However, Internet is not an unmixed blessing to the banking sector. Along with reduction in cost of transactions, it has also brought about a new orientation to risks and even new forms of risks to which banks conducting i-banking expose themselves. Regulators and supervisors all over the world are concerned that while banks should remain efficient and cost effective, they must be conscious of different types of risks this form of banking entails and have systems in place to manage the same. An important and distinctive feature is that technology plays a significant part both as source and tool for control of risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures. Both evolve continuously. The thrust of regulatory action in risk control has been to identify risks in broad terms and to ensure that banks have minimum systems in place to address the same and that such systems are reviewed on a continuous basis in keeping with changes in technology. In the following paragraphs a generic set of risks are discussed as the basis for formulating general risk control guidelines, which this Group will address.

5.2 Operational risk:

Operational risk, also referred to as transactional risk is the most common form of risk associated with i-banking. It takes the form of inaccurate processing of transactions, non enforceability of contracts, compromises in data integrity, data privacy and confidentiality, unauthorized access / intrusion to bank's systems and transactions etc. Such risks can arise out of weaknesses in design, implementation and monitoring of banks' information system. Besides inadequacies in technology, human factors like negligence by customers and employees, fraudulent activity of employees and crackers / hackers etc. can become potential source of operational risk. Often there is thin line of difference between operational risk and security risk and both terminologies are used interchangeably.

5.3 Security risk:

5.3.1 Internet is a public network of computers which facilitates flow of data / information and to which there is unrestricted access. Banks using this medium for financial transactions must, therefore, have proper technology and systems in place to build a secured environment for such transactions.

5.3.2 Security risk arises on account of unauthorized access to a bank's critical information stores like accounting system, risk management system, portfolio management system, etc. A breach of security could result in direct financial loss to the bank. For example, hackers operating via the Internet, could access, retrieve and use confidential customer information and also can implant virus. This may result in loss of data, theft of or tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service, cost of repairing these etc. Other related risks are loss of reputation, infringing customers' privacy and its legal implications etc. Thus, access control is of paramount importance. Controlling access to banks' system has become more complex in the Internet environment which is a public domain and attempts at unauthorized access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers. Also, in a networked environment the security is limited to its weakest link. It is therefore, necessary that banks critically assess all interrelated systems and have access control measures in place in each of them.

5.3.3 In addition to external attacks banks are exposed to security risk from internal sources e.g. employee fraud. Employees being familiar with different systems and their weaknesses become potential security threats in a loosely controlled environment. They can manage to acquire the authentication data in order to access the customer accounts causing losses to the bank.

5.3.4 Unless specifically protected, all data / information transfer over the Internet can be monitored or read by unauthorized persons. There are programs such as 'sniffers' which can be set up at web servers or other critical locations to collect data like account numbers, passwords, account and credit card numbers. Data privacy and confidentiality issues are relevant even when data is not being transferred over the net.

Data residing in web servers or even banks' internal systems are susceptible to corruption if not properly isolated through firewalls from Internet.

5.3.5 The risk of data alteration, intentionally or unintentionally, but unauthorized is real in a networked environment, both when data is being transmitted or stored. Proper access control and technological tools to ensure data integrity is of utmost importance to banks. Another important aspect is whether the systems are in place to quickly detect any such alteration and set the alert.

5.3.6 Identity of the person making a request for a service or a transaction as a customer is crucial to legal validity of a transaction and is a source of risk to a bank. A computer connected to Internet is identified by its IP (Internet Protocol) address. There are methods available to masquerade one computer as another, commonly known as 'IP Spoofing'. Likewise user identity can be misrepresented. Hence, authentication control is an essential security step in any e-banking system.

5.3.7 Non-repudiation involves creating a proof of communication between two parties, say the bank and its customer, which neither can deny later. Banks' system must be technologically equipped to handle these aspects which are potential sources of risk.

5.4 System architecture and design

5.4.1 Appropriate system architecture and control is an important factor in managing various kinds of operational and security risks. Banks face the risk of wrong choice of technology, improper system design and inadequate control processes. For example, if access to a system is based on only an IP address, any user can gain access by masquerading as a legitimate user by spoofing IP address of a genuine user. Numerous protocols are used for communication across Internet. Each protocol is designed for specific types of data transfer. A system allowing communication with all protocols, say HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), telnet etc. is more prone to attack than one designed to permit say, only HTTP.

5.4.2 Choice of appropriate technology is a potential risk banks face. Technology which is outdated, not scalable or not proven could land the bank in investment loss, a vulnerable system and inefficient service with attendant operational and security risks and also risk of loss of business.

5.4.3 Many banks rely on outside service providers to implement, operate and maintain their e-banking systems. Although this may be necessary when banks do not have the requisite expertise, it adds to the operational risk. The service provider gains access to all critical business information and technical systems of the bank, thus making the system vulnerable. In such a scenario, the choice of vendor, the contractual arrangement for providing the service etc., become critical components of banks' security. Bank should educate its own staff and over dependencies on these vendors should be avoided as far as possible.

5.4.4 Not updating bank's system in keeping with the rapidly changing technology, increases operational risk because it leaves holes in the security system of the bank. Also, staff may fail to understand fully the nature of new technology employed. Further, if updating is left entirely at customers' end, it may not be updated as required by the bank. Thus education of the staff as well as users plays an important role to avoid operational risk.

5.4.5 Approaches to reduce security related operational risk are discussed in detail in Chapter-6. These include access control, use of firewalls, cryptographic techniques, public key encryption, digital signature etc.

5.5 Reputational risk

5.5.1 Reputational risk is the risk of getting significant negative public opinion, which may result in a critical loss of funding or customers. Such risks arise from actions which cause major loss of the public confidence in the banks' ability to perform critical functions or impair bank-customer relationship. It may be due to banks' own action or due to third party action.

5.5.2 The main reasons for this risk may be system or product not working to the expectations of the customers, significant system deficiencies, significant security breach (both due to internal and external attack), inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if there are no alternative means of account access. Such situation may cause customer-discontinuing use of product or the service. Directly affected customers may leave the bank and others may follow if the problem is publicized.

5.5.3 Other reasons include losses to similar institution offering same type of services causing customer to view other banks also with suspicion, targeted attacks on a bank like hacker spreading inaccurate information about bank products, a virus disturbing bank's system causing system and data integrity problems etc.

5.5.4 Possible measures to avoid this risk are to test the system before implementation, back-up facilities, contingency plans including plans to address customer problems during system disruptions, deploying virus checking, deployment of ethical hackers for plugging the loopholes and other security measures.

5.5.5 It is significant not only for a single bank but also for the system as a whole. Under extreme circumstances, such a situation might lead to systemic disruptions in the banking system as a whole. Thus the role of the regulator becomes even more important as not even a single bank can be allowed to fail.

5.6 Legal risk

5.6.1 Legal risk arises from violation of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established.

5.6.2 Given the relatively new nature of Internet banking, rights and obligations in some cases are uncertain and applicability of laws and rules is uncertain or ambiguous, thus causing legal risk.

5.6.3 Other reasons for legal risks are uncertainty about the validity of some agreements formed via electronic media and law regarding customer disclosures and privacy protection. A customer, inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions.

5.6.4 In the enthusiasm of enhancing customer service, bank may link their Internet site to other sites also. This may cause legal risk. Further, a hacker may use the linked site to defraud a bank customer.

5.6.5 If banks are allowed to play a role in authentication of systems such as acting as a Certification Authority, it will bring additional risks. A digital certificate is intended to ensure that a given signature is, in fact, generated by a given signer. Because of this, the certifying bank may become liable for the financial losses incurred by the party relying on the digital certificate.

5.7 Money laundering risk

5.7.1 As Internet banking transactions are conducted remotely banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus banks expose themselves to the money laundering risk. This may result in legal sanctions for non-compliance with "know your customer" laws.

5.7.2 To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, conduct periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in Internet transactions.

5.8 Cross border risks

5.8.1 Internet banking is based on technology that, by its very nature, is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders. This causes various risks.

5.8.2 It includes legal and regulatory risks, as there may be uncertainty about legal requirements in some countries and jurisdiction ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risks associated with non-compliance of different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws.

5.8.3 If a bank uses a service provider located in another country, it will be more difficult to monitor it thus, causing operational risk. Also, the foreign-based service provider or foreign participants in Internet banking are sources of country risk to the extent that foreign parties become unable to fulfil their obligations due to economic, social or political factors.

5.8.4 Cross border transaction accentuates credit risk, since it is difficult to appraise an application for a loan from a customer in another country compared to a customer from a familiar customer base. Banks accepting foreign currencies in payment for electronic money may be subjected to market risk because of movements in foreign exchange rates.

5.9 Strategic Risk

5.9.1 This risk is associated with the introduction of a new product or service. Degree of this risk depends upon how well the institution has addressed the various issues related to development of a business plan, availability of sufficient resources to support this plan, credibility of the vendor (if outsourced) and level of the technology used in comparison to the available technology etc.

5.9.2 For reducing such risk, banks need to conduct proper survey, consult experts from various fields, establish achievable goals and monitor performance. Also they need to analyse the availability and cost of additional resources, provision of adequate supporting staff, proper training of staff and adequate insurance coverage. Due diligence needs to be observed in selection of vendors, audit of their performance and establishing alternative arrangements for possible inability of a vendor to fulfil its obligation . Besides this, periodic evaluations of new technologies and appropriate consideration for the costs of technological upgradation are required.

5.10 Other risks

5.10.1 Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk are also present in Internet banking. These risks get intensified due to the very nature of Internet banking on account of use of electronic channels as well as absence of geographical limits. However, their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational and legal risks. This may be particularly true for banks that engage in a variety of banking activities, as compared to banks or bank subsidiaries that specialize in Internet banking.

5.10.2 Credit risk is the risk that a counter party will not settle an obligation for full value, either when due or at any time thereafter. Banks may not be able to properly evaluate the credit worthiness of the customer while extending credit through remote banking procedures, which could enhance the credit risk. Presently, banks generally deal with more familiar customer base. Facility of electronic bill payment in Internet banking may cause credit risk if a third party intermediary fails to carry out its obligations with respect to payment. Proper evaluation of the creditworthiness of a customer and audit of lending process are a must to avoid such risk.

5.10.3 Another facility of Internet banking is electronic money. It brings various types of risks associated with it. If a bank purchases e-money from an issuer in order to resell it to a customer, it exposes itself to credit risk in the event of the issuer defaulting on its obligation to redeem electronic money,.

5.10.4 Liquidity Risk arises out of a bank's inability to meet its obligations when they become due without incurring unacceptable losses, even though the bank may ultimately be able to meet its obligations. It is important for a bank engaged in electronic money transfer activities that it ensures that funds are adequate to cover redemption and settlement demands at any particular time. Failure to do so, besides exposing the bank to liquidity risk, may even give rise to legal action and reputational risk.

5.10.5 Similarly banks dealing in electronic money face interest rate risk because of adverse movements in interest rates causing decrease in the value of assets relative to outstanding electronic money liabilities. Banks also face market risk because of losses in on-and-off balance sheet positions arising out of movements in market prices including foreign exchange rates. Banks accepting foreign currency in payment for electronic money are subject to this type of risk.

.**5.10.6** Risk of unfair competition: Internet banking is going to intensify the competition among various banks. The open nature of Internet may induce a few banks to use unfair practices to take advantage over rivals. Any leaks at network connection or operating system etc., may allow them to interfere in a rival bank's system.

5.11 Thus one can find that along with the benefits, Internet banking carries various risks for bank itself as well as banking system as a whole. The rapid pace of technological innovation is likely to keep changing the nature and scope of risks banks face. These risks must be balanced against the benefits. Supervisory and regulatory authorities are required to develop methods for identifying new risks, assessing risks, managing risks and controlling risk exposure. But authorities need to keep in consideration that the development and use of Internet banking are still in their early stages, and policies that hamper useful innovation and experimentation should be avoided. Thus authorities need to encourage banks to develop a risk management process rigorous and comprehensive enough to deal with known risks and flexible enough to accommodate changes in the type and intensity of the risks.

Chapter- 6- Technology and Security Standards For Internet Banking

6.1 Introduction

The Internet has provided a new and inexpensive channel for banks to reach out to their customers. It allows customers to access banks' facilities round the clock and 7 days a week. It also allows customers to access these facilities from remote sites/home etc. However, all these capabilities come with a price. The highly unregulated Internet provides a less than secure environment for the banks to interface. The diversity in computer, communication and software technologies used by the banks vastly increases the challenges facing the online bankers. In this chapter, an effort has been made to give an overview of the technologies commonly used in Internet banking. An attempt has been made to describe concepts, techniques and technologies related to privacy and security including the physical security. The banks planning to offer Internet banking should have explicit policies on security. An outline for a possible framework for security policy and planning has also been given. Finally, recommendations have been made for ensuring security in Internet banking.

6.2 Technologies

6.2.1 *Computer networking & Internet*

6.2.1.1 The purpose of computer networking is sharing of computing resources and data across the whole organization and the outside world. Computer Networks can be primarily divided into two categories based on speed of data transfers and geographical reach. A Local area network (LAN) connects many servers and workstations within a small geographical area, such as a floor or a building. Some of the common LAN technologies are 10 MB Ethernet, 100 MB Ethernet, 1GB Ethernet, Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM). The data transfer rates here are very high. They commonly use broadcast mode of data transfer. The Wide Area Network (WAN), on the other hand, is designed to carry data over great distances and are generally point-to-point. Connectivity in WAN set-up is provided by using dial-up modems on the Public Switched Telephone Network (PSTN) or leased lines, VSAT networks, an Integrated Services Digital Network (ISDN) or T1 lines, Frame Relay/X.25 (Permanent Virtual Circuits), Synchronous Optical Network

(SONET), or by using Virtual Private Networks (VPN) which are software-defined dedicated and customized services used to carry traffic over the Internet. The different topologies, technologies and data communication protocols have different implications on safety and security of services.

6.2.1.2 To standardize on communications between systems, the International Organization of Standards developed the OSI model (the Open System Interconnection Reference Model) in 1977. The OSI breaks up the communication process into 7 layers and describe the functions and interfaces of each layer. The important services provided by some of the layers are mentioned below. It is necessary to have a good understanding of these layers for developing applications and for deploying firewalls (described later).

Application Layer: Network Management, File Transfer Protocol, Information validation, Application-level access security checking.

Session Layer: establishing, managing and terminating connections (sessions) between applications

Transport Layer: Reliable transparent transfer of data between end points, end to end recovery & flow control.

Network Layer: Routing, switching, traffic monitoring and congestion control, control of network connections, logical channels and data flow.

Data Link Layer: Reliable transfer of data across physical link and control of flow of data from one machine to another.

6.2.1.3 *Protocols:* The data transmission protocol suite used for the Internet is known as the Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet is primarily a network of networks. The networks in a particular geographical area are connected into a large regional network. The regional networks are connected via a high speed "back bone". The data sent from one region to another is first transmitted to a Network Access Point (NAP) and are then routed over the backbone. Each computer connected to the Internet is given a unique IP address (such as 142.16.111.84) and a hierarchical domain name(such as cse.iitb.ernet.in).The Internet can be accessed using various application-level protocols such as FTP (File Transfer Protocol), Telnet (Remote Terminal Control Protocol), Simple Mail Transport Protocol (SMTP), Hypertext Transfer Protocol (HTTP). These protocols run on top of TCP/IP. The most innovative part of the Internet is the World Wide Web (WWW). The web uses hyperlinks, which allow users to move from any place on the web to any other place. The web consists of web pages, which are multimedia pages composed of text, graphics, sound and video. The web pages are made using Hypertext Markup Language (HTML). The web works on a client-server model in which the client software, known as the browser, runs on the local machine and the server software, called the web server, runs on a possibly remote machine. Some of the popular browsers are Microsoft Internet Explorer and Netscape Navigator.

6.2.1.4 With the popularity of web, organizations find it beneficial to provide access to their services through the Internet to its employees and the public. In a typical situation, a component of the application runs (as an 'applet') within the browser on user's workstation. The applet connects to the application (directly using TCP/IP or through web server using HTTP protocols) on the organization's application and database servers. These servers may be on different computer systems. The web-based applications provide flexible access from anywhere using the familiar browsers that support graphics and multimedia. The solutions are also scalable and easy to extend. Fig. 6.1 below shows some of the components and technologies/products commonly used in the design of web-based applications.

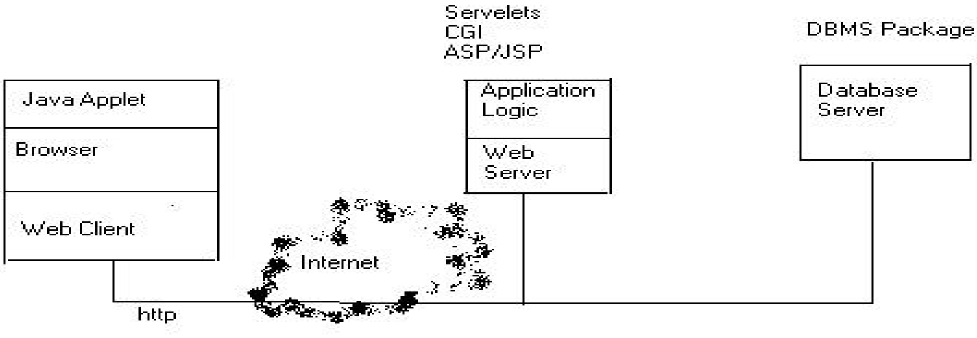

Fig. 6.1: Components of a web-based application

6.2.2 *Banking Products*: Internet Banking applications run on diverse platforms, operating systems and use different architectures. The product may support centralized (bank-wide) operations or branch level automation. It may have a distributed, client server or three tier architecture based on a file system or a DBMS package. Moreover, the product may run on computer systems of various types ranging from PCs, open (Unix based) systems, to proprietary main frames. These products allow different levels of access to the customers and different range of facilities. The products accessible through Internet can be classified into three types based on the levels of access granted:

1. **Information only systems**: General-purpose information like interest rates, branch locations, product features, FAQs, loan and deposit calculators are provided on the bank's web (WWW) site. The sites also allow downloading of application forms. Interactivity is limited to a simple form of 'e-mail'. No identification or authentication of customers is done and there is no interaction between the bank's production system (where current data of accounts are kept and transactions are processed) and the customer.
2. **Electronic Information Transfer System***:* These systems provide customer-specific information in the form of account balances, transaction details, statement of account etc. The information is still largely 'read only'. Identification and authentication of customer takes place using relatively simple techniques (like passwords). Information is fetched from the Bank's production system in either the batch mode or offline. Thus, the bank's main application system is not directly accessed.
3. **Fully Transactional System**: These systems provide bi-directional transaction capabilities. The bank allows customers to submit transactions on its systems and these directly update customer accounts. Therefore, security & control system need to be strongest here.

6.2.3 Application architecture

A computer-based application may be built as a monolithic software, or may be structured to run on a client–server environment, or even have three or multi-tiered architecture. A computer application typically separates its 3 main tasks: interactions with the user, processing of transactions as per the business rules, and the storage of business data. The three tasks can be viewed as three layers, which may run on the same system (possibly a large, proprietary computer system), or may be separated on to multiple computers (across the Internet), leading to three-tier or multi-tier architecture. These layers can be briefly described as follows:

1. Presentation Layer: This layer is responsible for managing the front-end devices, which include browsers on personal computers, Personal Digital Assistants (PDAs), mobile phones, Internet kiosks, Web TV etc. The presentation layer takes care of user interface related issues like display details, colour, layout, image etc. It also has important responsibilities in user authentication and session management activity.
2. Application layer: It contains the business logic (for processing of data and transactions) and necessary interfaces to the data layer. It processes requests from the presentation layer, connects to the data layer, receives and processes the information and passes results back to the presentation layer. It is responsible for ensuring that all the business rules are incorporated in the software. The issues of scalability, reliability and performance of the services to a great extent depend upon the application layer architecture.
3. Data Layer: The data layer uses a database package to store, retrieve and update application data. The database may be maintained on one or multiple servers. A database package also supports back-up and recovery of data, as well as logging of all transactions.

6.2.4 *Issues in administration of systems and applications***:** The role of the network and the database administrator is pivotal in securing the information systems of any organization. The role extends across various job functions and any laxity in any of the functions leaves the system open for malicious purposes. A few important functions of the administrator and how they relate to or impinge on system security are discussed below:

a. *Installation of software:* A software (whether system or application) needs to be carefully installed as per the developer's instructions. The software system may contain bugs and security holes, which over a period are fixed through appropriate patches. It is necessary to know the latest and correct configuration of all software packages. Hackers and intruders are often aware of these bugs and may exploit known weaknesses in the software; hence, care should be taken to install only the latest versions of software with the latest patches. Further, improper installation may lead to degradation of services. Installation of pirated software is not only illegal and unethical, but may also contain trojans and viruses, which may compromise system security. In the case of installation of outsourced software, care should be taken to compare the source code and the executable code using appropriate tools as unscrupulous developers may leave backdoor traps in the software and for illegal access and update to the data. In addition, while installing software care should be taken that only necessary services are enabled on a need to use basis.

b. *Access controls and user maintenance* **:** An administrator has to create user accounts on different computer systems, and give various access permissions to the users. Setting access controls to files, objects and devices reduces intentional and unintentional security breaches. A bank's system policy should specify access privileges and controls for the information stored on the computers. The administrators create needed user groups and assign users to the appropriate groups. The execution privilege of most system–related utilities should be limited to system administrators so that users may be prevented from making system level changes. The write / modify access permissions for all executables and binary files should be disabled. If possible, all log files should be made "append only". All sensitive data should be made more secure by using encryption. The system and database administrators are also responsible for the maintenance of users and the deletion of inactive users. Proper logs should be maintained of dates of user creation and validity period of users. There should be a frequent review to identify unnecessary users and privileges, especially of temporary users such as system maintenance personnel and system auditors.

c. *Backup, recovery & business continuity***:** Back-up of data, documentation and software is an important function of the administrators. Both data and software should be backed up periodically. The frequency of back up should depend on the recovery needs of the application. Online / real time systems require frequent backups within a day. The back-up may be incremental or complete. Automating the back up procedures is preferred to obviate operator errors and missed back-ups. Recovery and business continuity measures, based on criticality of the systems, should be in place and a documented plan with the organization and assignment of responsibilities of the key decision making personnel should exist. An off-site back up is necessary for recovery from major failures / disasters to ensure business continuity. Depending on criticality, different technologies based on back up, hot sites, warm sites or cold sites should be available for business continuity. The business continuity plan should be frequently tested.

4. *System & network logging* : Operating systems, database packages and even business applications produce a 'log' of various tasks performed by them. Most operating systems keep a log of all user actions. Log files are the primary record of suspicious behavior. Log files alert the administrator to carry out further investigation in case of suspicious activity and help in determining the extent of intrusion. Log files can also provide evidence in case of legal proceedings. The administrator has to select types of information to be logged, the mechanisms for logging, locations for logging, and locations where the log files are stored. The information required to be logged should include Login/Logout information, location and time of failed attempts, changes in status, status of any resource, changes in system status such as shutdowns, initializations and restart; file accesses, change to file access control lists, mail logs, modem logs, network access logs, web server logs, etc. The log files must be protected and archived regularly and securely.

6.3 Security and Privacy Issues

6.3.1 *Terminology:*

1. *Security:* Security in Internet banking comprises both the computer and communication security. The aim of computer security is to preserve computing resources against abuse and unauthorized use, and to protect data from accidental and deliberate damage, disclosure and modification. The communication security aims to protect data during the transmission in computer network and distributed system.
2. *Authentication:* It is a process of verifying claimed identity of an individual user, machine, software component or any other entity. For example, an IP Address identifies a computer system on the Internet, much like a phone number identifies a telephone. It may be to ensure that unauthorized users do not enter, or for verifying the sources from where the data are received. It is important because it ensures authorization and accountability. Authorization means control over the activity of user, whereas accountability allows us to trace uniquely the action to a

specific user. Authentication can be based on password or network address or on cryptographic techniques.

3. *Access Control:* It is a mechanism to control the access to the system and its facilities by a given user up to the extent necessary to perform his job function. It provides for the protection of the system resources against unauthorized access. An access control mechanism uses the authenticated identities of principals and the information about these principals to determine and enforce access rights. It goes hand in hand with authentication. In establishing a link between a bank's internal network and the Internet, we may create a number of additional access points into the internal operational system. In this situation, unauthorized access attempts might be initiated from anywhere. Unauthorized access causes destruction, alterations, theft of data or funds, compromising data confidentiality, denial of service etc. Access control may be of discretionary and mandatory types.
4. *Data Confidentiality:* The concept of providing for protection of data from unauthorized disclosure is called data confidentiality. Due to the open nature of Internet, unless otherwise protected, all data transfer can be monitored or read by others. Although it is difficult to monitor a transmission at random, because of numerous paths available, special programs such as "Sniffers", set up at an opportune location like Web server, can collect vital information. This may include credit card number, deposits, loans or password etc. Confidentiality extends beyond data transfer and include any connected data storage system including network storage systems. Password and other access control methods help in ensuring data confidentiality.
5. *Data Integrity:* It ensures that information cannot be modified in unexpected way. Loss of data integrity could result from human error, intentional tampering, or even catastrophic events. Failure to protect the correctness of data may render data useless, or worse, dangerous. Efforts must be made to ensure the accuracy and soundness of data at all times. Access control, encryption and digital signatures are the methods to ensure data integrity.
6. *Non-Repudiation:* Non-Repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that data

has been received or to protect the recipient against false denial by the sender that the data has been sent. To ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communication or transaction.

7. *Security Audit Trail:* A security audit refers to an independent review and examination of system's records and activities, in order to test for adequacy of system controls. It ensures compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in the control, policy and procedures. Audit Trail refers to data generated by the system, which facilitates a security audit at a future date.

6.3.2 *Attacks and Compromises:*

When a bank's system is connected to the Internet, an attack could originate at any time from anywhere. Some acceptable level of security must be established before business on the Internet can be reliably conducted. An attack could be any form like:

1. The intruder may gain unauthorized access and nothing more
2. The intruder gains access and destroys, corrupt or otherwise alters data
3. The intruder gains access and seizes control partly or wholly, perhaps denying access to privileged users
4. The intruder does not gain access, but instead forges messages from your system
5. The intruder does not gain access, but instead implements malicious procedures that cause the network to fail, reboot, and hang.

Modern security techniques have made cracking very difficult but not impossible. Further more, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security hole. A wide range of information regarding security hole and their fixes is freely available on the Internet. System administrator should keep himself updated with this information.

Common cracking attacks include:

1. E-mail bomb and List linking
2. Denial-of-Service
3. Sniffer attack

4. Utilizing security hole in the system software

5. *E-mail bomb:* This is a harassment tool. A traditional e-mail bomb is simply a series of message (perhaps thousands) sent to your mailbox. The attacker's object is to fill the mailbox with junk.
6. *Denial-of-Service (DoS) attacks:* DoS attacks can temporarily incapacitate the entire network(or at least those hosts that rely on TCP/IP). DoS attacks strike at the heart of IP implementations. Hence they can crop up at any platform, a single DoS attack may well work on several target operating systems. Many DoS attacks are well known and well documented. Available fixes must be applied.
7. *Sniffer Attack***:** Sniffers are devices that capture network packets. They are a combination of hardware and software. Sniffers work by placing the network interface into promiscuous mode. Under normal circumstances, all machines on the network can "hear" the traffic passing through, but will only respond to data addressed specifically to it. Nevertheless, if the machine is in promiscuous mode then it can capture all packets and frames on the network. Sniffers can capture passwords and other confidential information. Sniffers are extremely difficult to detect because they are passive programs. Encrypted session provides a good solution for this. If an attacker sniffs encrypted data, it will be useless to him. However, not all applications have integrated encryption support.
8. *Holes:* A hole is any defect in hardware, software or policy that allows attackers to gain unauthorized access to your system. The network tools that can have holes are Routers, Client and Server software, Operating Systems and Firewalls.

6.3.3 Authentication Techniques:

As mentioned earlier, authentication is a process to verify the claimed identity. There are various techniques available for authentication. Password is the most extensively used method. Most of the financial institutions use passwords along with PIN (Personal Identification Number) for authentication. Technologies such as tokens, smart cards and biometrics can be used to strengthen the security structure by requiring the user to possess something physical.

1. *Token* technology relies on a separate physical device, which is retained by an individual, to verify the user's identity. The token resembles a small hand-held

card or calculator and is used to generate passwords. The device is usually synchronized with security software in the host computer such as an internal clock or an identical time based mathematical algorithm. Tokens are well suited for one-time password generation and access control. A separate PIN is typically required to activate the token.

2. *Smart cards* resemble credit cards or other traditional magnetic stripe cards, but contain an embedded computer chip. The chip includes a processor, operating system, and both Read Only Memory (ROM) and Random Access Memory (RAM). They can be used to generate one-time passwords when prompted by a host computer, or to carry cryptographic keys. A smart card reader is required for their use.
3. *Biometrics* involves identification and verification of an individual based on some physical characteristic, such as fingerprint analysis, hand geometry, or retina scanning. This technology is advancing rapidly, and offers an alternative means to authenticate a user.

6.3.4 Firewalls :

The connection between internal networks and the outside world must be watched and monitored carefully by a gatekeeper of sorts. Firewalls do this job. Otherwise, there is a risk of exposing the internal network and systems, often leaving them vulnerable and compromising the integrity and privacy of data. Firewalls are a component or set of components that restrict access between a protected network and the outside world (i.e., the Internet). They control traffic between outside and inside a network, providing a single entry point where access control and auditing can be imposed. All firewalls examine the pieces or packets of data flowing into and out of a network and determine whether a particular person should be given access inside the network. As a result, unauthorized computers outside the firewall are prevented from directly accessing the computers inside the internal network. Broadly, there are three types of firewalls i.e. Packet filtering firewalls, Proxy servers and stateful inspection firewall.

- *Packet filtering routers:*

Packet filtering routers are the simplest form of firewalls. They are connected between the host computer of an Internal network and the Internet gateway as shown in Fig.6. 2. The bastion host directs message accepted by the router to the appropriate application servers in the protected network. Their function is to route data of a network and to allow only certain types of data into the network by checking the type of data and its source and destination address. If the router determines that the data is sourced from an Internet address which is not on its acceptable or trusted sources list, the connection would be simply refused. The advantage of this type of firewall is that it is simple and cheaper to implement and also fast and transparent to the users. The disadvantage is that if the security of the router were compromised, computers on the internal network would be open to external network for attacks. Also, the filtering rules can be difficult to configure, and a poorly configured firewall could result in security loopholes by unintentionally allowing access to an internal network.

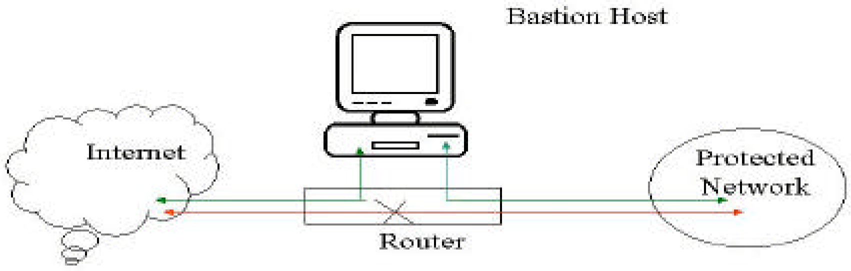

Fig. 2 : A filtering router with a bastion host or proxy server

- *Proxy servers:*

Proxy servers control incoming and outgoing traffic for a network by executing specific proxy program for each requested connection. If any computer outside the internal network wants to access some application running on a computer inside the internal network, then it would actually communicate with the proxy server, and proxy server in turn will pass the request to the internal computer and get the response which will be given to the recipient (outside user). That is, there is no direct connection between the internal network and Internet. This approach allows a high level of control and in-depth monitoring using logging and auditing tools. However, since it doubles the amount of processing, this approach may lead to som degradation in performance. Fig. 3 shows a typical firewall organization consisting of 'militarized zone' that separates the protected network from the Internet.

a.   Stateful Inspection firewall:

This type of firewalls thoroughly inspects all packets of information at the network level as in the case of proxy servers. Specifications of each packet of data, such as the user and the transportation method, the application used are all queried and verified in the inspection process. The information collected is maintained so that all future transmissions are inspected and compared to past transmission. If both the "state" of the transmission and the "context" in which it is used deviate from normal patterns, the connection would be refused. This type of firewalls are very powerful but performance would also decline due to the intensive inspection and verification performed.

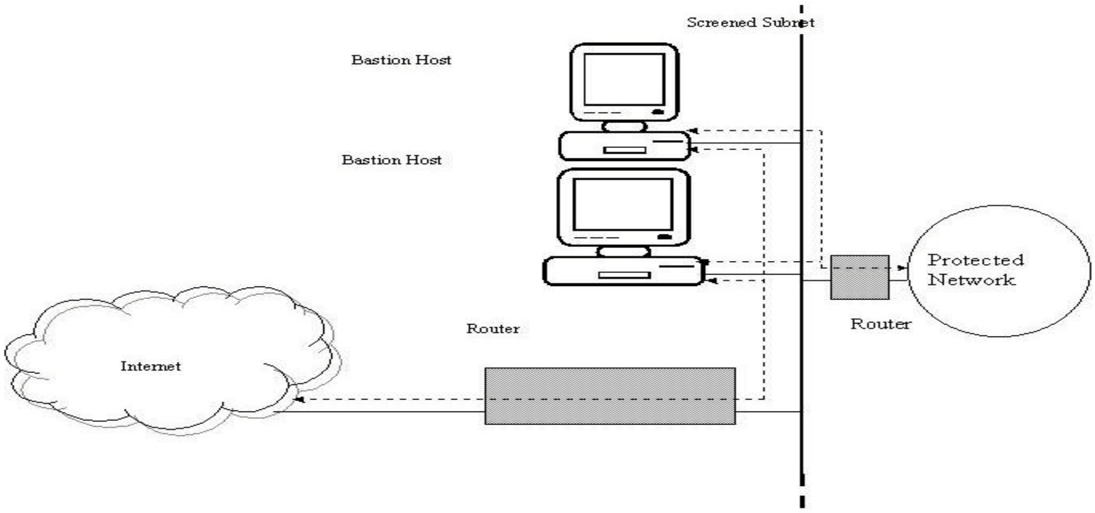

Fig.6.3 : Creating a 'Militarized Zone" to protect internal systems

6.3.5 *Cryptography*:

The process of disguising a message in such a way as to hide its substance is called encryption. An encrypted message is called cipher text. The process of turning a cipher text back into plain text is called decryption. Cryptography is the art and science of keeping messages secure. It uses a 'key' for encrypting or decrypting a message. Both the method of encryption and the size of key are important to ensure confidentiality of a message. There are two types of encryption: Symmetric key and Asymmetric key encryption. In the symmetric key cryptography scheme, the same key is used to encrypt and decrypt the message. Common symmetric algorithms include One-time pad encryption, Data Encryption Standard (DES), Triple DES, LOKI, Twofish, Blowfish, International Data Encryption Algorithm (IDEA). DES and Triple DES are the commonly used techniques. Asymmetric key cryptography scheme is also known as Public key crypto-system. Here two keys are used. One key is kept secret and therefore it is referred as "private key". The other key is made widely available to anyone who wants it, and is referred as "Public key". The Public key and Private key are mathematically related so that information encrypted using the public key can only be decrypted by the corresponding private key and vice-versa. Importantly, it is near to impossible to find out the private key from the public key. Common and more popular public key cryptosystem algorithms are Diffie-Hellman, RSA, Elliptic Curve etc. In all these, the confidentiality is directly related to the key size. Larger the key size, the longer it takes to break the encrypted message.

- *Diffie-Hellman*: This is the first public key algorithm invented. It gets its security from the difficulty of calculating discrete logarithms in a finite field. Diffie-Hellman method can be used for distribution of keys to be used for symmetric encryption.
- *RSA:* Named after its three inventors, Ron Rivest, Adi Shamir and Leonard Adleman, who first introduced the algorithm in 1978, RSA gets its security from the difficulty of factoring large numbers. The public and private keys are function of a pair of large (100 or 200 digits or even larger) prime numbers. The pair is used for asymmetric encryption.

6.3.6 *Digital Signature and certification:*

6.3.6.1 Digital signatures authenticate the identity of a sender, through the private, cryptographic key. In addition, every digital signature is different because it is derived from the content of the message itself. The combination of identity authentication and singularly unique signatures results in a transmission that can not be repudiated.

6.3.6.2 Digital signature can be applied to any data transmission, including e-mail. To generate digital signature, the original, unencrypted message is processed through mathematical algorithms that generate a ‘message digest’ (a unique character representation of data). This process is known as “hashing”. The message digest is then encrypted with the private key and sent along with the message (could be encrypted also). The recipient receives both the message and encrypted message digest. The recipient decrypts the message digest using the sender’s public key, and then runs the message through the hash function again. If the resulting message digest matches the one sent with the message, the message has not been altered and data integrity is verified. Because the message digest was encrypted using the private key, the sender can be identified and bound to the specific message.

6.3.6.3 *Certification Authorities and Digital Certificates:*

Certificate Authorities and Digital Certificates are emerging to further address the issues of authentication, non-repudiation, data privacy and cryptographic key management. A Certificate Authority (CA) is a trusted third party that verifies the identity of a party to a transaction. To do this, the CA vouches for the identity of a party by attaching the CA’s digital signature to any messages, public keys, etc., which are transmitted. The CA must be trusted by the parties involved, and identities must have been proven to the CA beforehand. Digital certificates are messages that are signed with the CA’s private key. They identify the CA, the represented party, and even include the represented party’s public key.

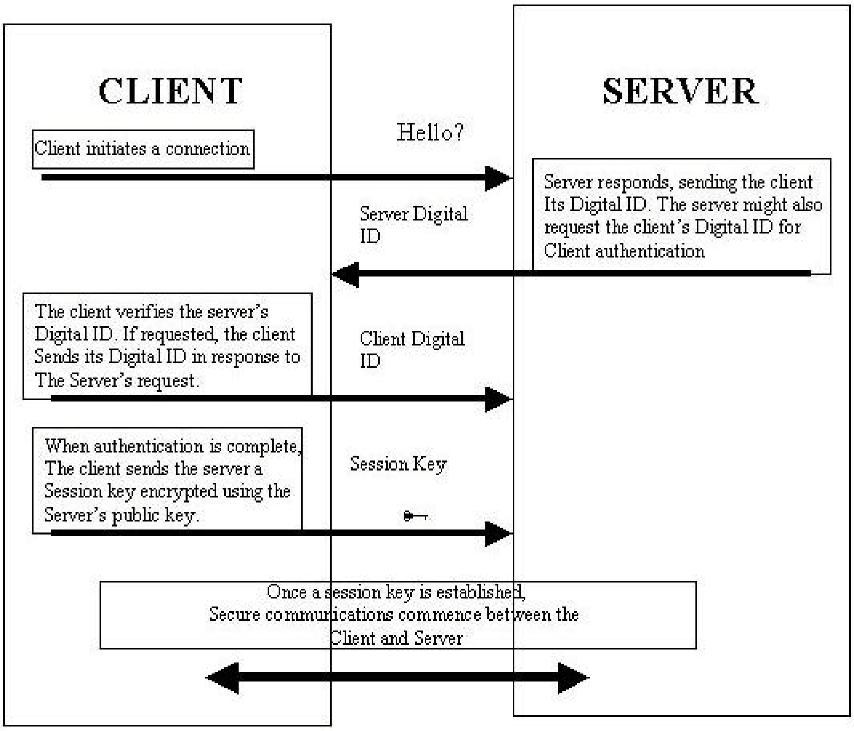
CLIENT
SERVER
Hello?
Client initiates a connection
Server responds, sending the client Its Digital ID. The server might also request the client's Digital ID for Client authentication
Server Digital ID
The client verifies the server's Digital ID. If requested, the client Sends its Digital ID in response to The Server's request.
Client Digital ID
When authentication is complete, The client sends the server a Session key encrypted using the Server's public key.
Session Key
Once a session key is established, Secure communications commence between the Client and Server

Fig.6.4 : Flow of messages in SSL-based security (at conceptual level)

6.3.6.4 *Secure Socket Layer (SSL)*:

SSL is designed to make use of TCP to provide a reliable end-to-end secure service. The SSL servers have digital certificates issued by Certifying Authorities so that the clients can authenticate the service provider (a bank in our case). The servers use a password /PIN/digital certificate to authenticate clients. Once the clients and server have authenticated each other, they establish a session key for encryption of messages. The diagram above shows flow of messages in SSL. The flow of authentication messages in SSL is shown in Fig.6.4.

6.3.7 *Public Key Infrastructure (PKI):*

6.3.7.1 Public key cryptography can play an important role in providing needed security services including confidentiality, authentication, digital signatures and integrity. Public key cryptography uses two electronic keys: a public key and a private key. The public key can be known by anyone while the private key is kept secret by its owner. As long as there is strong binding between the owner and the owner's public key, the identity of the originator of a message can be traced to the owner of the private key. A Public Key Infrastructure (PKI) provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable Certification Authority (CA).

6.3.7.2 PKI consists of the following components :

b. *Key Certificate* - An electronic record that binds a public key to the identity of the owner of a public-private key pair and is signed by a trusted entity.

c. *Certification Authority (CA)* - A trusted entity that issues and revokes public key certificates

d. *Registration Authority (RA)* - An entity that is trusted by the CA to register or vouch for the identity of users to the CA.

e. *Certificate Repository* - An electronic site that holds certificates and CRLs. CAs post certificates and CRLs to repositories.

f. *Certificate Revocation List (CRL)* - A list of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example, a certificate can be revoked if the owner's private key has been lost or if the owner's name changes**.**

g. *Certificate User* - An entity that uses certificates to know, with certainty, the public key of another entity.

6.3.7.3 The widespread use of PKI technology to support digital signatures can help increase confidence of electronic transactions. For example, the use of a digital signature allows a seller to prove that goods or services were requested by a buyer and therefore demand payment. The use of a PKI allows parties without prior knowledge of each other to engage in verifiable transactions.

6.3.7.4 *Confidentiality and PKI :* A PKI could also support confidentiality services using a public-private key pair that is different from the one used for signing. In this case, users need to obtain a separate certificate for the confidentiality public key. To send an encrypted message, a user could obtain the recipient's confidentiality certificate from a certificate repository and verify that it is valid. Then the sender can encrypt the message using the public key. Only the recipient, in possession of the private key, will be able to decrypt the message.

6.3.7.5 *Certificates* **:** Although there have been several proposed formats for public key certificates, most certificates available today are based on an international standard (ITU-T X.509 version 3). This standard defines a certificate structure that includes several optional extensions. The use of X.509v3 certificates is important because it provides interoperability between PKI components. Also, the standard's defined extensions offer flexibility to support specific business needs.

6.3.7.6 *PKI Architectures:*

A PKI is often composed of many CAs linked by trust paths. The CAs may be linked in several ways. They may be arranged hierarchically under a "root CA" that issues certificates to subordinate CAs. The CAs can also be arranged independently in a network. Recipients of a signed message with no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate. The National Institute of Standards and Technology (NIST) has developed a hybrid architecture specification based on both a hierarchical and a network architecture model in the document, Public Key Infrastructure (PKI) Technical Specifications (Version 2.3): Part C - Concept of Operations.

6.3.8 *Tools:*

Tools are extremely useful in monitoring and controlling networks, systems and users. Some of the system administration and network management tools are Scanners, Sniffers, Logging and Audit tools.

a. *Scanners:* Scanners query the TCP/IP port and record the target's response and can reveal the information like services that are currently running, users owning those services, whether anonymous logins are supported, and whether certain network services require authentication. Scanners are important because they reveal weaknesses in the network. There are many security vulnerabilities on any given platform. Scanners can do an excellent security audit and then system can be suitably upgraded. Scanners are programs that automatically detect security weaknesses in remote or local hosts. System administrators may use them to find out weaknesses in their system and take preventive measures. Scanners can be used to gather preliminary data for an audit. Scanners offer a quick overview of TCP/IP security.

b. *Sniffer:* Sniffers are devices that capture network packets. They analyze network traffic and identify potential areas of concern. For example, suppose one segment of the network is performing poorly. Packet delivery seems incredibly slow or machines inexplicably lock up on a network boot. Sniffers can determine the precise cause. Sniffers are always a combination of hardware and software components. Proprietary sniffers are generally expensive (vendors often package them on special computers that are “optimized “ for sniffing).

c. *Intrusion Detection Tools:* An intrusion attempt or a threat is defined to be the potential possibility of a deliberate unauthorized attempt to access or manipulate information or render a system unreliable or unusable. Different approaches are used to detect these intrusion attempts. Some Intrusion Detection Systems (IDS) are based on audit logs provided by the operating system i.e. detecting attacks by watching for suspicious patterns of activity on a single computer system. This type of IDS called Host based IDS is good at discerning attacks that are initiated by local users which involve misuse of the capabilities of one system. The Host based IDS can interpret only high level logging information and they can not detect low level network events such as Denial of Service attacks. The network-based approach can be effectively used to detect these low level Denial of Service attacks. Distributed intrusion detection systems (DIDS) take data from various hosts, network components and network monitors and try to detect intrusions from the collected data**.**

d. Network based Intrusion Detection Systems (NIDS) are based on interpretation of raw network traffic. They attempt to detect attacks by watching for patterns of suspicious activity in this traffic. NIDS are good at discerning attacks that involve low-level manipulation of the network, and can easily correlate attacks against multiple machines on a network. An Intrusion Detection System detects the attacks in real-time and informs system administrator about it to take appropriate action. As a result, exposure to the intrusion and the possible damage caused to the data or systems can be countered.

6.3.9 *Physical Security:*

6.3.9.1 Physical security is a vital part of any security plan and is fundamental to all security efforts--without it, information security, software security, user access security, and network security are considerably more difficult, if not impossible, to initiate. Physical security is achieved predominantly by controlled and restricted physical access to the systems resources. *Access control* broadly provides the ability to grant selective access to certain people at certain times and deny access to all others at all times. Physical security involves the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes and accidental damage (e.g., from electrical surges, extreme temperatures and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Thus, in broad terms, the focus is on restricting access to the computer area, controlling access to all vulnerable and sensitive areas of the department, and monitoring of all staff and visitors.

6.3.9.3 Physical Access can be secured through the following means: Bolting Door locks and Combination Locks, Electronic Door Locks, Biometric Door Locks, Manual Logging, Electronic Logging, Photo Identification Badges, Video Cameras stationed at strategic points, Controlled Visitor Access. A bank should also have in place environmental controls to manage exposures from fire, natural disasters, power failure, air-conditioning failure, water damage, bomb threat / attack etc. A few means of obtaining control over environmental exposure are:

1. The server room and any other unattended equipment room should have water detector. Fire extinguishers should be placed at all strategic points, supplementing fire suppression systems with smoke detectors, use of fire resistant materials in office materials including furniture, redundant power supply from two substations, electrical wiring placed in fire resistant panels and conduits and documented and tested evacuation plans.
2. It is important to educate all ‘stake-holders’ (users, employees, etc) about the importance of physical security. This education should be carried out as part of ‘social engineering’.

6.3.10 *Security Policy:*

6.3.10.1 The information security policy is the systemization of approaches and policies related to the formulation of information security measures to be employed within the organization to assure security of information and information systems owned by it. The security policy should address the following items:

1. Basic approach to information security measures.
2. The information and information systems that must be protected, and the reasons for such protection.
3. Priorities of information and information systems that must be protected.
4. Involvement and responsibility of management and establishment of an information security coordination division.
5. Checks by legal department and compliance with laws / regulations.
6. The use of outside consultants.
7. Identification of information security risks and their management.
8. Impact of security policies on quality of service to the customers (for example, disabling an account after three unsuccessful logins may result in denial of service when it is done by somebody else mischievously or when restoration takes unduly long time).
9. Decision making process of carrying out information security measures.
10. Procedures for revising information security measures.
11. Responsibilities of each officer and employee and the rules (disciplinary action etc) to be applied in each case.
12. Auditing of the compliance to the security policy.
13. User awareness and training regarding information security.
14. Business continuity Plans.
15. Procedures for periodic review of the policy and security measures.

6.3.10.2 The top management of the bank must express a commitment to security by manifestly approving and supporting formal security awareness and training. This may require special management level training. Security awareness will teach people not to disclose sensitive information such as password file names. Security guidelines, policies and procedures affect the entire organization and as such, should have the support and suggestions of end users, executive management, security administration, IS personnel and legal counsel.

6.4 Recommendations

6.4.1 *Security Organization:* 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.

6.4.2 *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.

6.4.3 *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.

6.4.4 *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.

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

1. Usage of SSL, which ensures server authentication and the use of client side 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.

6.4.6 *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.

6.4.7 *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.

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

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 Hackers').

6.4.9 *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.

6.4.10 *Back up & 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.

6.4.11 *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.

6.4.12 *Education & 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.

6.4.13 *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.)

6.4.14 *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).

6.4.15 *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.

6.4.16 *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. RBI may call for various documents pertaining to security, reliability, availability, auditability, recoverability, and other important aspects of the services. RBI may provide model documents for Security Policy, Security Architecture, and Operations Manual.

6.4.17 *Standing Committee:* RBI may set up a standing Committee to monitor security policy issues and technologies, to review prescribed standards, and to make fresh recommendations on a regular basis.

Chapter -7 - Legal Issues involved in Internet Banking

7.1.1 The legal framework for banking in India is provided by a set of enactments, viz., the Banking Regulations Act, 1949, the Reserve Bank of India Act, 1934, and the Foreign Exchange Management Act, 1999. Broadly, no entity can function as a bank in India without obtaining a license from Reserve Bank of India under Banking Regulations Act, 1949. Different types of activities which a bank may undertake and other prudential requirements are provided under this Act. Accepting of deposit from public by a non-bank attracts regulatory provisions under Reserve Bank of India Act 1934. Under the Foreign Exchange Management Act 1999, no Indian resident can lend, open a foreign currency account or borrow from a non resident, including non-resident banks, except under certain circumstances provided in law. Besides these, banking activity is also influenced by various enactments governing trade and commerce, such as, Indian Contract Act, 1872, the Negotiable Instruments Act, 1881, Indian Evidence Act, 1872, etc.

7.1.2 As discussed earlier, Internet banking is an extension of the traditional banking, which uses Internet both as a medium for receiving instructions from the customers and also delivering banking services. Hence, conceptually, various provisions of law, which are applicable to traditional banking activities, are also applicable to Internet banking. However, use of electronic medium in general and Internet in particular in banking transactions, has put to question the legality of certain types of transactions in the context of existing statute. The validity of an electronic message / document, authentication, validity of contract entered into electronically, non-repudiation etc. are important legal questions having a bearing on electronic commerce and Internet banking. It has also raised the issue of ability of banks to comply with legal requirements / practices like secrecy of customers account, privacy, consumer protection etc. given the vulnerability of data / information passing through Internet. There is also the question of adequacy of law to deal with situations which are technology driven like denial of service / data corruption because of technological failure, infrastructure failure, hacking, etc. Cross border transactions carried through Internet pose the issue of jurisdiction and conflict of laws of different nations.

7.1.3 This dichotomy between integration of trade and finance over the globe through e-commerce and divergence of national laws is perceived as a major obstacle for e-commerce / i-banking and has set in motion the process of harmonization and standardization of laws relating to money, banking and financial services. A major initiative in this direction is the United Nations Commission on International Trade Law (UNICITRAL)'s Model law, which was adopted by the General Assembly of United Nations and has been recommended to the member nations for consideration while revising / adopting their laws of electronic trade.

7.1.4 Government of India has enacted The Information Technology Act, 2000, in order *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'…*The Act, which has also drawn upon the Model Law, came into force with effect from October 17, 2000. The Act has also amended certain provisions of the Indian Penal Code, the Indian Evidence Act, 1872, The Bankers Book of Evidence Act, 1891 and Reserve Bank of India Act 1934 in order to facilitate e-commerce in India. However, this Act will not apply to:-

1. A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
2. A power-of-attorney as defined in section 1A of the Power-of-Attorney Act, 1882;
3. A trust as defined in section 3 of the Indian Trusts Act, 1882;
4. A will as defined in clause (*h*) of section 2 of the Indian Succession Act, 1925;
5. Any contract for the sale or conveyance of immovable property or any interest in such property;
6. Any such class of documents or transactions as may be notified by the Central Government in the official Gazette.

7.1.5 In the course of providing Internet banking services the banks in India are facing new challenges relating to online opening of accounts, authentication, secrecy of customers accounts, non-repudiation, liability standards and consumer protection, etc., each of which has been examined in the context of existing legal framework.

7.2.1 *Online opening of account:* The banks providing Internet banking service, at present are only willing to accept the request for opening of accounts. The accounts are opened only after proper physical introduction and verification. This is primarily for the purpose of proper identification of the customer and also to avoid benami accounts as also money laundering activities that might be undertaken by the customer. Supervisors world over, expect the Internet banks also to follow the practice of 'know your customer'.

7.2.2 As per Section 131 of the Negotiable Instruments Act, 1881 (the Act) a banker who has in good faith and without negligence received payment for a customer of a cheque crossed generally or specially to himself shall not, in case the title to the cheque proves defective, incur any liability to the true owner of the cheque by reason only of having received such payment. The banker's action in good faith and without negligence have been discussed in various case laws and one of the relevant passages from the judgment of Justice Chagla in the case of Bapulal Premchand Vs Nath Bank Ltd. (AIR 1946 Bom.482) is as follows:

"Primarily, inquiry as to negligence must be directed in order to find out whether there is negligence in collecting the cheque and not in opening the account, but if there is any antecedent or present circumstance which aroused the suspicion of the banker then it would be his duty before he collects the cheque to make the necessary enquiry and undoubtedly one of the antecedent circumstances would be the opening of the account. In certain cases <u>failure to make enquiries as to the integrity of the proposed customer would constitute negligence".</u>

7.2.3 Further the Supreme Court of India in Indian Overseas Bank Ltd. Vs. Industrial Chain Concern [JT1989(4)SC 334] has stated that as a general rule, before accepting a customer, the bank must take reasonable care to satisfy himself that <u>the person in question is in good reputation</u> and if he fails to do so, he will run the risk of forfeiting the protection given by Section 131 of Negotiable Instruments Act, 1881 but reasonable care depends upon the facts and circumstances of the case. Similarly, the Delhi High Court was also of the view that the modern banking practice requires that a constituent should either be known to the bank or should be properly introduced. The underlying object of the bank insisting on producing reliable references is only to find out if possible <u>whether the new constituent is a genuine party or an imposter or a</u>

fraudulent rogue [Union of India Vs National Overseas Grindlays Bank Ltd. (1978) 48 Com.Cases 277 (Del)].

7.2.4 Thus, the introduction of a new customer by a third party reference is a well-recognized practice followed by the banks before opening new accounts in order to prove the reasonable care and absence of any negligence in permitting the new customer to open the account. Further, in order to establish the reasonable care the banks have to make enquiries about the integrity/reputation of the prospective customer. It is not a mere enquiry about the identity of the person. The Group, therefore, endorses the practice presently followed by the banks in seeking proper introduction before allowing the operations of the customers' accounts. In the context of Internet banking and after the coming into force of the Information Technology Act, 2000, it may be possible for the banks to rely on the electronic signatures of the introducer. But this may have to await till the certification machinery as specified in the Information Technology Act, 2000 comes into operation.

7.3.1 *Authentication:* One of the major challenges faced by banks involved in Internet banking is the issue relating to authentication and the concerns arising in solving problems unique to electronic authentication such as issues of data integrity, non-repudiation, evidentiary standards, privacy, confidentiality issues and the consumer protection. The present legal regime does not set out the parameters as to the extent to which a person can be bound in respect of an electronic instruction purported to have been issued by him. Generally, authentication is achieved by what is known as security procedure. Methods and devices like the personal identification numbers (PIN), code numbers, telephone-PIN numbers, relationship numbers, passwords, account numbers and encryption are evolved to establish authenticity of an instruction. From a legal perspective, the security procedure requires to be recognized by law as a substitute for signature. Different countries have addressed these issues through specific laws dealing with digital signatures. In India, the Information Technology Act, 2000 (the "Act") in Section 3 (2) provides that any subscriber may authenticate an electronic record by affixing his digital signature. However the Act only recognizes one particular technology as a means of authenticating the electronic records (viz, the asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record). This might lead to the doubt of whether the law would recognize the existing methods used by the banks as a valid method of authenticating the transactions. In this regard as noted in paragraph [3.2.2] of Chapter [3] of this Report, the approach in the other countries has been to keep the legislation technology neutral. The Group is of the view that the law should be technology neutral so that it can keep pace with the technological developments without requiring frequent amendments to the law as there exists a lot of uncertainty about future technological and market developments in Internet banking. This however would not imply that the security risks associated with Internet banking should go unregulated.

7.3.2 Hence, Section 3 (2) of the Information Technology Act 2000 may need to be amended to provide that the authentication of an electronic record may be effected either by the use of the asymmetric crypto system and hash function, or a system as may be mutually determined by the parties or by such other system as may be prescribed or approved by the Central Government. If the agreed procedure is followed by the parties concerned it should be deemed as being an authenticate transaction. A clarification to this effect by way of an amendment of the aforesaid Act will facilitate the Internet banking transactions.

7.3.3 Further, the banks may be allowed to apply for a license to issue digital signature certificate under Section 21 of the Information Technology Act, 2000 and become a certifying authority for facilitating Internet banking. The certifying authority acts like a trusted notary for authenticating the person, transaction and information transmitted electronically. Using a digital certificate from trusted certificate authority like a bank shall provide a level of comfort to the parties of an Internet banking transaction. Hence, it is recommended by the Committee that the Reserve Bank of India may recommend to the Central Government to notify the business of the certifying authority under Clause (o) of Section 6(1) of the Banking Regulation Act, 1949, to permit the banks to act as such trusted third parties in e-commerce transactions.

7.4.1 *Mode of Payment under the Income Tax Act, 1961:* Section 40A(3) of the Income tax Act, 1961, dealing with deductible expenses, provides that in cases where the amount exceeds Rs. 20,000/-, the benefit of the said section will be available only if the payment is made by a crossed cheque or a crossed bank draft. One of the services provided by the banks offering Internet banking service is the online transfer of funds between accounts where cheques are not used, in which the above benefit will not be available to the customers.

7.4.2 The primary intention behind the enactment of Section 40 A of the Income tax Act, 1961 is to check tax evasion by requiring payment to designated accounts. In the case of a funds transfer, the transfer of funds takes place only between identified accounts, which serves the same purpose as a crossed cheque or a crossed bank draft. Hence, the Committee recommends that Section 40A of the Income Tax Act, 1961, may be amended to recognise even electronic funds transfer.

7.5.1. *Secrecy of Customer's Account:* The existing regime imposes a legal obligation on the bankers to maintain secrecy and confidentiality about the customer’s account. The law at present requires the banker to take scrupulous care not to disclose the state of his customer's account except on reasonable and proper occasions.[1]

7.5.2. While availing the Internet banking services the customers are allotted proper User ID, passwords and/or personal identification numbers and/or the other agreed authentication procedure to access the Internet banking service and only users with such access methodology and in accordance with the agreed procedure are authorized to access the Internet banking services. In other words a third party would not be able to withdraw money from an account or access the account of the customer unless the customer had divulged his/her password in the first place.

7.5.3 However, if the password or the identification number is misplaced or lost or gets into the hands of the wrong person and such person procures details about the customers account then the banker may be faced with legal proceedings on the grounds of violation of the obligation to maintain secrecy of the customer's accounts. This concern of the bankers is very high especially in the case of joint accounts where both the parties share one personal identification numbers or relationship numbers and operate the account jointly. Further, by the very nature of Internet the account of a customer availing Internet banking services would be exposed to the risk of being accessed by hackers and inadvertent finders.

7.5.4 The Internet banking services at present are being provided by most of the banks by

[1] *Tournier v. National Provincial and Union Bank of England*, (1924) 1 K.B. 461

systems which are only accessible through "secure zones" or SSL (Secure Sockets Layer) to secure and authenticate the user through a secure browser. Most of the banks have adopted 128 Bit strong encryption which is widely accepted worldwide as a standard for securing financial transaction. To reduce the risk of the customers' account information being accessed by third parties, it is very important that the banks continue to be obliged to protect the customer account. However, it is equally important to note that the banks may still be exposed to the risk of liability to customers and hence they should adopt all reasonable safety controls and detection measures like establishment of firewalls, net security devices, etc. Further, banks should put in place adequate risk control measures in order to minimize possible risk arising out of breach of secrecy due to loss/ misplacement/ theft of customers' ID/PIN, etc.

7.6.1 *Revocation and Amendment of Instructions:* The general revocation and amendment instructions to the banks are intended to correct errors, including the sending of an instruction more than once. Occasionally, a revocation or amendment may be intended to stop a fraud. Under the existing law, banks are responsible for making and stopping payment in good faith and without negligence. In an Internet banking scenario there is very limited or no stop-payment privileges since it becomes impossible for the banks to stop payment in spite of receipt of a stop payment instruction as the transactions are completed instantaneously and are incapable of being reversed. Hence the banks offering Internet banking services may clearly notify the customers the time frame and the circumstances in which any stop payment instructions could be accepted**.**

7.7.1 *Rights and Liabilities of the Parties:* Typically, the banker-customer relationship is embodied in a contract entered into by them. The banks providing the Internet banking services currently enter into agreements with their customers stipulating their respective rights and responsibilities including the disclosure requirements in the case of Internet banking transactions, contractually. A Standard format/minimum consent requirement to be adopted by the banks offering Internet banking facility, could be designed by the Indian Banks' Association capturing, inter alia, access requirements, duties and responsibilities of the banks as well as customers and any limitations on the liabilities of the banks in case of negligence and non-adherence to the terms of agreement by customers.

7.8.1. *Internet Banking and Money Laundering:*

One of the major concerns associated with Internet Banking has been that the Internet banking transactions may become untraceable and are incredibly mobile and may easily be anonymous and may not leave a traditional audit trail by allowing instantaneous transfer of funds. It is pertinent to note that money-laundering transactions are cash transactions leaving no paper trail**.** Such an apprehension will be more in the case of use of electronic money or e-cash. In the case of Internet Banking the transactions are initiated and concluded between designated accounts. Further Section 11 of the proposed Prevention of Money Laundering Bill, 1999 imposes an obligation on every Banking Company, Financial Institution and intermediary to maintain a record of all the transactions or series of transactions taking place within a month, the nature and value of which may be prescribed by the Central Government. These records are to be maintained for a period of five years from the date of cessation of the transaction between the client and the banking company or the financial institution or the intermediary. This would apply to banks offering physical or Internet banking services. This will adequately guard against any misuse of the Internet banking services for the purpose of money laundering. Further the requirement of the banking companies to preserve specified ledgers, registers and other records for a period of 5 to 8 years, as per the Banking Companies (Period of Preservation of Records) Rules, 1985 promulgated by the Central Government also adequately takes care of this concern.

7.9.1. *Maintenance of Records:* Section 4 of the Bankers' Books Evidence Act, 1891, provides that a certified copy of any entry in a banker's book shall in all legal proceedings be received as a prima facie evidence of the existence of such an entry. The Banking Companies (Period of Preservation of Records) Rules, 1985 promulgated by the Central Government requires banking companies to maintain ledgers, records, books and other documents for a period of 5 to 8 years. A fear has been expressed as to whether the above details of the transactions if maintained in an electronic form will also serve the above purpose. The Group is of the considered opinion that that this has been adequately taken care of by Section 7 and Third Schedule of the Information Technology Act, 2000.

7.10.1 *Inter-Bank Electronic Funds Transfer:* The Electronic Funds Transfer via the Internet, in its present form is provided only between accounts with the same bank. The transaction is effected by the originator who gives the electronic payment order to one branch of a bank offering the Internet banking facility ("the Sending Branch"). The electronic instruction is processed by the backend software of the branch to confirm the account number and the person's identification and instruction is issued by the Sending Branch to the branch having the account of the beneficiary ("Beneficiary Branch") to credit the account of the beneficiary. The Sending Branch debits the account of the originator at its end. At present there is no clearing mechanism in place for settlement of inter-bank electronic funds transfer. The entire gamut of electronic funds transfer and the legal issues and risks involved in the same are currently being examined by a committee set up by the Reserve Bank of India. The 4th Schedule to the Information Technology Act, 2000 has amended the Reserve Bank of India Act. 1934 empowering the Reserve Bank of India to regulate electronic funds transfer between banks and banks and other financial institutions.

7.11.1 *Miscellaneous:* During the course of deliberations, the Group discussed certain issues where the legal position is not clear but have a bearing on Internet banking. Certain issues have also not been addressed by the Information Technology Act, 2000. Such issues are briefly discussed below. The Consumer Protection Act 1986 defines the rights of consumers in India and is applicable to banking services as well. The issues of privacy, secrecy of consumers' accounts and the rights and liabilities of customers and banks, etc. in the context of Internet banking have been discussed in earlier paragraphs. In cases where bilateral agreements defining customers rights and liabilities are adverse to consumers than what are enjoyed by them in the traditional banking scenario, it is debatable whether such agreements are legally tenable. For example, whether a bank can claim immunity if money is transferred unauthorizedly by a hacker from a customers account, on the pretext that it had taken all reasonable and agreed network security measures. In a traditional banking scenario, a bank has normally no protection against payment of a forged cheque. If the same logic is extended, the bank providing I-banking may not absolve itself from liability to the customers on account of unauthorized transfer through hacking. Similar position may obtain in case of denial of service. Even though, The Information Technology Act, 2000 has provided for penalty for denial of access to a computer system (Section-43) and hacking (Section – 66), the liability of banks in such situations is not clear. The Group was of the view that the banks providing Internet banking may assess the risk and insure themselves against such risks.

7.11.2 There was no specific enactment in India which protects privacy of customers. Bankers' secrecy obligation mostly followed from different case laws. In UK, the Data Protection Act 1984 specifically prohibits personal data from being disclosed for purposes other than for which the data is held. This prohibits use of customer data relating to their spending habits, preferences etc., for any commercial purpose. The Office of the Comptroller of Currency have also issued directions to US banks enforcing customers' privacy. The Information Technology Act, 2000, in Section 72 has provided for penalty for breach of privacy and confidentiality. Further, Section 79 of the Act has also provided for exclusion of liability of a network service provider for data travelling through their network subject to certain conditions. Thus, the liability of banks for breach of privacy when data is travelling 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.

7.11.3 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.

Chapter- 8- Regulatory and supervisory concerns

8.1 Banking on the Internet provides benefits to the consumer in terms of convenience, and to the provider in terms of cost reduction and greater reach. The Internet itself however is not a secure medium, and thus poses a number of risks of concern to regulators and supervisors of banks and financial institutions. World over, regulators and supervisors are still evolving their approach towards the regulation and supervision of Internet banking. Regulations and guidelines issued by some countries include the following.

1. Requirement to notify about web site content
2. Prior authorization based on risk assessment made by external auditors
3. On-site examination of third party service providers
4. Off-site policing the perimeters to look for infringement.
5. Prohibition on hyper links to non bank business sites
6. Specification of the architecture

In some countries supervisors have followed a 'hands-off' approach to regulation of such activities, while others have adopted a wait and watch attitude. This chapter suggests approaches to supervision of Internet banking activities, drawing upon the best international practices in this area as relevant to the Indian context.

8.2 Major supervisory concerns

8.2.1 These concerns can be clubbed into the following:

1. Operational risk issues
2. Cross border issues
3. Customer protection and confidentiality issues
4. Competitiveness and profitability issues

8.2.2 *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.

8.2.3 *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 Potentiality 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 centres, records or back up centres 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.

8.2.4 *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.

8.2.5 *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.

8.3 Broad regulatory framework

It would be necessary to extend the existing regulatory framework over banks to Internet banking also. Such an approach would need to take into account the provisions of both the Banking Regulation Act 1949 and the Foreign Exchange Management Act, 1999.

1. Only such banks which are licensed and supervised in India and have a physical presence here should be permitted to offer Internet banking products to residents of India.
2. These products should be restricted to account holders only and should not be offered in other jurisdictions.
3. The services should only offer local currency products and that too by entities who are part of the local currency payment systems.
4. The ‘in-out’ scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the ‘out-in’ scenario where Indian residents are offered banking services by banks operating in cross-border jurisdictions are generally not permitted and this approach should be carried over to Internet banking also.
5. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., would however be permitted transactions.
6. Overseas branches of Indian banks would be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor in keeping with the supervisory approach outlined in

the next section.

7. This extension of approach would apply to virtual banks as well. Thus, both banks and virtual banks incorporated outside the country and having no physical presence here would not, for the present, be permitted to offer Internet services to Indian depositors.

8.4 Recommendations

With the above approach in mind, the Group recommends that the regulatory and supervisory concerns relating to Internet banking can be met in the manner outlined in the following paragraphs.

8.4.1 All banks which propose to offer transactional services on the Internet should obtain an in-principle approval from RBI prior to commencing these services. The application should be accompanied by a note put up to the Board of the bank along with Board resolution passed. The Board note should cover the reasons for the bank choosing to enter into such business, the potential penetration it seeks to achieve, a cost-benefit analysis, a listing of products it seeks to offer, the technology and business partners for the products, and all third party support services and service providers with their track record and agreements with them, and the systems and the skills and capabilities it has in this regard and most materially the systems, controls and procedures it has put or intends to put in place to identify and manage the risks arising out of the proposed ventures. The bank should also enclose a security policy framed in this regard which should cover all the recommendations made in Chapter 6 of this report and produce a certification from a reputed external auditor who is CISA or otherwise appropriately qualified that the security measures taken by the bank are adequate and meet the requirements and that risk management systems are in place to identify and mitigate the risks arising out of the entire gamut of Internet banking operations.

8.4.2 The RBI could require the bank together with the auditor to hold discussions with the RBI in this regard before granting such approval. After this initial approval is given, the bank would be obliged to inform the RBI of any material changes in web-site content and launch of new products.

8.4.3 The assurance about security controls and procedures, which is sought from the specialist external auditors, should be periodically obtained, with the periodicity depending on the risk assessment of the supervisor. Further, banks would also be required to report every breach or failure of the security systems and procedures to RBI, who may decide to subject the failure to an on-site examination or even commission an auditor to do so.

8.4.4 The RBI as supervisor would cover the entire risks associated with electronic banking as part of its annual inspections. For this purpose, a checklist could be developed along the lines of those covering general computerized banking featured in the manual developed for inspection of computerized branches. Till such time as the RBI builds up sufficient capability to do this in-house, it is recommended that this function be outsourced to qualified EDP auditors.

8.4.5 The focus of the supervisory approach would mainly be the transactional Internet banking services offered by existing banks as an alternative channel. To some extent the concerns in this regard are the same as those arising out of electronic banking in general. The RBI has issued guidelines in the recent past on the "Risks and Controls in Computers and Telecommunications" which would be applicable equally to Internet banking. Another supervisory focus would be on Record Maintenance and their availability for inspection and audit. Again, RBI has issued guidelines for these "Preservation and Record Maintenance" which need to be updated to include the risks heightened by banking on the net. Broadly, the record preservation and maintenance policy must encompass record keeping, record retention, record media and record location. The key features of this enhancement would be as follows:

1. The cornerstone of this policy should be security. Access to all bank-related electronic data should be restricted to authorized individuals.

2. All transactional, financial and managerial data pertaining to the previous financial year must be archived before 1 July of the subsequent financial year.

3. A senior officer / executive of the Bank possessing appropriate qualifications, education and/or background should be designated in-charge of the archived data. A possible designation could be Archived Data Security Officer.

4. All access to archived data should be with the authentic (written or by e-mail) approval of this Archived Data Security Officer (ADSO).

5. The role and responsibilities of the ADSO should be clearly delineated and well

publicized within the bank.

6. Data so archived should be on such a platform and using such a technology that future alteration / modification / deletion of the data is not possible, once the data is archived.

7. If the technology and/or platform used for data storage involves compression and/or dis-aggregation of data, banks should have in place adequate software/hardware which will ensure easy restoration of the data as and when required by the bank's own departments and also by RBI as well as other statutory authorities.

8. All transactional, financial and managerial data should be available on-line. If, for reasons of paucity of on-line storage, such data (of the current financial year) has been backed-up and removed from on-line storage, it must be available in a format and at a location which ensures that the data can be restored on-line within a maximum of 24 hours from the date and time at which the demand for such data is made by users from within the bank or from RBI or other statutory authorities.

9. Similarly, transactional, financial and managerial data of the previous financial year should be made available within a maximum of 48 hours of the date and time at which such request is made by the bank's own users or by the RBI and other statutory authorities.

8.4.6 A vulnerability which is accentuated in Internet banking is the reliance upon third party providers and support services and this requires banks to effectively manage the risks of all outsourced activities. In turn the supervisors should have the ability to assess the risks arising out of such liaisons. **Direct supervision of the third party by the supervisor is not envisaged. Accordingly, as part of the Internet policy, banks should develop outsourcing guidelines, which mitigate the risks of disruption and defective service. Alternatively, the IBA (Indian Banks Association) or IDRBT (Institute for Development and Research in Banking Technology) could be asked to develop broad guidelines for the use of the banking community.**

8.4.7 *Payment Gateway:*

8.4.7.1 An externally shared service, which will develop, as the pivot of the Internet banking would be the payment gateway. With the increasing popularity of "e-Commerce" i.e., buying and selling over the Internet, electronic payments and settlements for such purchases, is a natural and expected requirement. Banks, which are the vital segment of the payment system in the country, will therefore be required to equip themselves to meet this emerging challenge. In its basic form, the 'Inter-Bank Payment Gateway' for payments and settlements of e-Commerce transactions is not very different from the traditional cheque clearing system, which is perhaps the most widely prevalent form of Inter-Bank settlement of funds, or the net settlement system of the international card agencies like Visa, Master Cards and American Express, for the credit card payments.

8.4.7.2 With the emergence of the Internet and the ability to buy and sell over the Internet, it has become imperative to deploy a similar Inter-Bank Payment Gateway to facilitate authorization for payments and settlement between participating institutions for commercial transactions carried out over the Internet. No one particular model for setting up an Inter-Bank Payment Gateway for such payments has been established as yet and we are, therefore, in a situation where the regulatory and supervisory framework itself needs to be evolved.

8.4.7.3 Given the above considerations, the following framework for setting up Inter-Bank Payment Gateways for Internet payments in India is suggested:

1. Only institutions that are members of the cheque clearing system in the country may be permitted to participate in the Inter-Bank Payment Gateway initiatives for Internet payments.
2. Both 'net-settlement' and 'gross-settlement' capabilities might be necessary, net settlement being the settlement mode for transaction below a certain pre-specified threshold value and gross settlement for transactions higher than the pre-specified value.
3. The Inter-Bank Payment Gateway should have one nominated bank as the clearing bank to settle all transactions.
4. The approval for setting up the Inter-Bank Payment Gateway should be granted only by the Reserve Bank of India, in their capacity as the Regulator of banks and Payment Systems in the country. The norms to become eligible to set up the Inter-Bank Payment Gateway should be specified by the Reserve Bank of India, on the basis of which institutions may seek formal approval to set up the Inter-Bank Payment Gateway.

5. It is expected that there will not be more than two or three Inter Bank Payment Gateways in the Country and all banks who wish to participate in the payment and settlement for e-Commerce transactions originated over the Internet could become a member of one or more of these Inter-Bank Payment Gateways.

6. All payments routed through the Inter-Bank Gateways should only cover direct debits and direct credits to the accounts maintained with the participating Banks by the parties involved in the e-Commerce transaction.

7. Payments effected using credit cards should not be routed through the Inter-Bank Payment Gateway. These should be authorized by the payer bank (i.e., acquiring bank) directly through its credit card authorization capability.

8. It should be obligatory on the part of the Inter-Bank Payments Gateway to establish, at any time, the complete trace of any payment transactions routed through it. The trace should cover date and time stamp when the transaction was originated and authorized, the payee details (account number and name of the payee bank), the payers details (account number and name of the payer bank), as well as a unique Transactional Reference Number (TRN) provided by both the Payee Bank and Payer Bank for each transaction.

9. Connectivity between the Inter-Bank Payment Gateway and the computer system of the member Banks should be achieved using a leased line network (not over the Internet), with appropriate data encryption standards.

10. All settlements over the Inter-Bank Payment Gateway should be intra-day, as far as possible in real time.

11. Until the exchange control aspects with regard to cross-border issues of e-Commerce transactions are fully discussed and documented, payment and settlement of such transactions should not be permitted over the Inter-Bank Payment Gateway.

12. Only Inter Bank Payments and Settlements (i.e. transactions involving more than one Bank) should be routed through the Inter-Bank Payment Gateway. Intra-bank payments (i.e., transactions involving only one Bank) should be handled by the bank’s own internal system.

13. The responsibility for the credit risk associated with every payment transaction routed over the Inter Bank Payment Gateway will rest with the appropriate Payee

Bank.

14. The mandate and the related documentation (that would form the basis for effecting payments for transactions carried out over the Internet) should be bilateral in nature i.e., (a) between the Payee and the Payee's bank (b) the Payer and Payer's bank, (c) between the participating banks and the service provider who is responsible for the operations of the Inter Bank Payment Gateway, and (d) between the banks themselves who are participating in the Inter Bank Payment Gateway Initiative. The rights and obligations of each party should be clearly stated in the mandate and should be valid in a court of law.

15. All transactions must be authenticated using a user ID and password. SSL/128 bit encryption must be used as the minimum level of security. As and when the regulatory framework is in place, all such transactions should be digitally certified by one of the licensed Certification Authorities.

16. The Service Provider who is responsible for the operations of the Inter-Bank Payment Gateway must ensure adequate firewalls and related security measure to ensure privacy to the participating institution, i.e., every institution can access data pertaining to only itself and its customer transactions.

17. Internationally accepted standards such as ISO8583 must be used for transmitting payment and settlement messages over the Network.

18. It may also be appropriate to have a panel of approved Auditors who will be required to certify the security of the entire infrastructure both at the Inter-Bank Payment Gateway as well as the participating institution's end prior to making the facility available for customer use. A process of perpetual audit must also be instituted.

8.4.8 It is not enough for the risk identification and assessment exercise to be between the bank and the supervisor alone. The customer too needs to be enlightened of the risks inherent in doing business on the net, and this would be served by having a mandatory disclosure template which would list the risks to the customer and the responsibilities and possible liability of the banks and the customer. Banks should also provide their most recent published financial results on their web-site.

8.4.9 The issue of reputation risk due to customers misunderstanding the hyper-links on the web-sites of banks also needs to be addressed. Fundamentally there are two scenarios where hyperlinks are necessary between non-bank business sites and bank-sites:

1. Where the Bank is required to inform visitors to its own Web Site about the Portals with whom they have a payment arrangement or Portals that the bank would want its customers to visit. These out-bound hyperlinks are unlikely to have any major security implications to the bank. In order to reflect the stability of the banking system, banks should not be seen as sponsors of or promoters of the products of unrelated businesses or of any businesses, which they are not licensed to run. The hyperlinks should hence be confined to only those portals with which they have a payment arrangement or the sites of their subsidiaries or principals.

2. The second type of hyperlink is where the Portal sites link to the bank site to pass information pertaining to a payment by one of their Internet Shoppers. This usually involves making a URL (Universal Resource Locator) link to the bank site to request authorization for payment. Such links deliver to the bank site information regarding the customer (typically his registration no) and the value of the payment to be authorized. Unless the bank exercises the right level of authentication and security, this type of URL links can be the source of a number of security breaches. It is therefore imperative that every bank ensures at least the following minimum-security precautions in order that the bank's as well as its customer’s interests are protected.

8.4.9.1 Upon receiving the URL request from the Portal site, the bank should authenticate the customer who has originated the transaction by asking him to key in, on the browser screen, his user ID and password which the bank would have provided him to facilitate access to his accounts with the bank.

8.4.9.2 Upon such authentication and due verification, the bank should re-submit the transaction information on the customer’s browser terminal i.e., the name of the Portal site to whom the payment is to be effected as well as the value of the transactions and seek the explicit approval of the customer to authorize the payment.

8.4.9.3 Depending on the nature of the payment, the payment authorization request should be routed either to the credit card authorizing system if payment is requested using credit card, or to the banks’ host system in case of a direct debit or to the Inter-Bank Payment Gateway in case of debit to customer account in another bank.

8.4.9.4 Upon receiving the payment authorization, the bank should return the URL request to the originating Portal, with a unique reference number for the transaction, as a conformation to pay as per the settlement cycle agreed with the Portal.

8.4.9.5 All interactions with the Portal sites as well as the customers browser terminal should be secured using SSL/128 bit encryption as a minimum requirement and should in due course be also augmented with the digital certification requirement as and when digital certificate deployment is enabled in the country.

8.5 It was deliberated whether banks undertaking Internet banking should be subject to any additional capital charge because of the potentially higher proneness to unexpected losses. As yet standards have not been developed for measuring additional capital charge on account of operational risks. However, this will be covered in a way once the banks move towards risk-based supervision where supervisory intervention will be linked to the risk profile of individual institutions. In such a scenario, an enhanced supervisory risk assessment on this account could warrant an additional capital charge, which would also be consistent with the second pillar approach of the new capital accord.

8.6 The Basle 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 will identify the areas of concern for supervision of cross border e-banking activities and will promote cooperative international efforts within the banking industry. It will evolve sound practices and will encourage and facilitate 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.

Chapter–9 - Recommendations

Keeping in view the terms of reference, the Group has made a number of recommendations in preceding chapters. A summary of these recommendations is given below.

9.1 Technology and Security Standards:

9.1.1 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-vis 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, business continuity plan is in place and frequently tested and there is a robust system of keeping log of all network activity and analyzing the same.

(Para 6.2.4)

9.1.2 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.

(Para 6.3.10, 6.4.1)

9.1.3 *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.

(Para 6.4.2)

9.1.4 *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.

(Para 6.4.3)

9.1.5 *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.

(Para 6.4.4)

9.1.6 *Security Infrastructure:* PKI is the most favoured technology for secure Internet banking services. However, it is not yet commonly available. While PKI infrastructure is strongly recommended, during the transition period, 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 side 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.

(Para 6.4.5)

9.1.7 *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.

(Para 6.4.6)

9.1.8 *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.

(Para 6.4.7)

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

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 Hackers').

(Para 6.4.8)

9.1.10 *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.

(Para 6.4.9)

9.1.11 *Back up & 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.

(Para 6.4.10)

9.1.12 *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. (Para 6.4.11)

9.1.13 *Education & 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. (Para 6.4.12)

9.1.14 *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.)

(Para 6.4.13)

9.1.15 *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).

(Para 6.4.14)

9.1.16 *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.

(Para 6.4.15)

9.1.17 *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, auditability, recoverability, and other important aspects of the services. RBI may provide model documents for Security Policy, Security Architecture, and Operations Manual.

(Para 6.4.16)

9.2 Legal Issues

9.2.1 The banks providing Internet banking service, 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 laws, the Group holds the view that there is an obligation on the banks not only to establish the identity 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. (Para 7.2.1)

9.2.2 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, personal identification number (PIN), code numbers and encryption etc., used to establish authenticity of an instruction. However, from a legal perspective a security procedure needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. This has raised the doubt whether the law would recognize the existing methods used by banks as valid methods of authentication. The Group holds the view that as in case of other countries, the law should be technology neutral.

(Para 7.3.1)

9.2.3 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 to by the concerned parties should be recognized as a valid method of authentication of an electronic document / transaction during the transition period.

(Para 7.3.2)

9.2.4 Banks may be allowed to apply for a license to issue digital signature certificate under Section 21 of the Information Technology Act, 2000 and function as certifying authority for facilitating Internet banking. Reserve Bank of India may recommend to Central Government for notifying the business of certifying authority as an approved activity under clause (o) of Section 6(1) of the Banking Regulations Act, 1949.

(Para 7.3.3)

9.2.5 Section 40A(3) of the Income Tax Act, 1961 recognizes only payments through a crossed cheque or crossed bank draft, where such payment exceeds Rs. 20000/-, 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.

(Para 7.4.2)

9.2.6 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 service etc., because of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risk.

(Para 7.5.1-7.5.4)

9.2.7 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.

(Para 7.6.1)

9.2.8 The banks providing Internet banking service and customers availing of the same are currently entering into agreements defining respective rights and liabilities in respect of Internet banking 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.

(Para 7.7.1)

9.2.9 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.

(Para 7.8.1)

9.2.10 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 a computer system (Section-43) and hacking (Section – 66), the liability of banks in such situations is not clear. The Group was of the view that the banks providing Internet banking may assess the risk and insure themselves against such risks.

(Para 7.11.1)

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

(Para 7.11.2)

9.3 Regulatory and Supervisory Issues

9.3.1 All banks, which propose to offer transactional services on the Internet should obtain approval from RBI prior to commencing these services. Bank's application for such permission should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners and third party service providers and systems 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 an 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.

(Para 8.4.1, 8.4.2)

9.3.2 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.

(Para 8.4.3)

9.3.3 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.

(Para 8.4.4, 8.4.5)

9.3.4 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 risks heightened by banking on the net. The enhancements will 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 alteration 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.

(Para 8.4.6)

9.3.5 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.

(Para 8.4.7)

9.3.6 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 institution should seek RBI's approval for setting up the same.

(Para 8.4.7, 8.4.9.1 – 8.4.9.5)

9.3.7 Only institutions who are members of the cheque 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 intra-bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway.

(Para 8.4.7)

9.3.8 Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as far 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 of origin of transaction, payee, payer and a unique transaction reference number (TRN).

(Para 8.4.7)

9.3.9 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.

(Para 8.4.7)

9.3.10 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.

(Para8.4.7)

9.3.11 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.

(Para 8.4.7)

9.3.12 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.

(Para 8.4.9)

9.3.12 Hyperlinks from banks' 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 from a banks' websites should be confined to only those portals with which they have a payment arrangement or sites of their subsidiaries or principals. Hyperlinks to banks' website from different portals are normally meant to pass information pertaining to purchases made by banks' 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.

(Para 8.4.10)

9.3.14 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.

(Para 8.5)

9.3.15 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.

(Para 7.11.3, 6.4.17)

9.3.16. 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 Basle 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.

(S. R. Mittal)
Chairman

(M. R. Srinivasan)
Member

(Prof N. L. Sarda)
Member

(S. H. Bhojani)
Member

(Romesh Sobti)
Member

(K. R. Ganapathy)
Member

(Deepak Ghaisas)
Member

(Ravi Nair)
Member

(K. M. Shettigar)
Member

(M. P. Kothari)
Member Secretary

Annexure-1

Note in respect of Liability of Banks

I have perused the draft report of the working group on Internet banking ('the Report").

I would like to express my disagreement on the following issues:

1. In Paragraph 6.4.16 of the Report it has been provided that that any bank offering internet banking services has to first obtain the approval of the Reserve Bank of India. In this regard I would like to submit that internet banking is merely an extension of the traditional banking activities. Section 6 of the Banking Regulation Act, 1949 does not make a distinction between the banking transactions carried traditionally and that over the Internet. Therefore no separate authorisation or prior approval of the regulator is required for the banks to offer internet banking facilities, since it is the same banking activities being carried out by the banks by way of adoption of different means and medium.

   I appreciate and understand that the intention of the Working Group in providing for the same has been to ensure that there are no security breaches while providing the internet banking services. Security breaches may either be due to certain inherent defects in the technology or due to the weaknesses in the design, implementation or monitoring of the system and cannot be controlled or avoided by a prior approval process. I am of the view that security breaches can be controlled and avoided to a great extent by periodic security risk assessment and inspection by the Reserve Bank of India and the internal management of the Bank providing such facility and by stipulating certain minimum security policy and infrastructure standards which a bank providing internet banking activity has to adopt. Further it should also be noted that prior approval process as envisaged in the Report may expose the Reserve Bank of India to the onerous liability in case there is any security breach after a prior approval has been provided by the Reserve Bank of India.

2. In Paragraph 7.1 1.1, an example has been cited as to whether a bank can claim immunity if money is transferred unauthorisedly by a hacker from a customers' account, on the pretext that it had taken all reasonable and agreed network security measures. It further cites that in a traditional banking scenario, a bank has normally no protection against payment of a forged cheque, and that if the same logic is extended, the bank providing internet banking may not absolve itself from liability to the customers on account of unauthorized transfer through hacking.

Hacking would involve someone gaining unauthorized access, to a communication between the banker and customer that may contain commercial terms, secrets or credit details, for the purpose of either intentionally changing the contents of the communication to prejudice the interests of the parties to the communication, or using the information for some other illegal use. The essence of hacking is to cause a breach in the established network security protocols and measures. An act of hacking is intensely a technological issue, and may be perpetrated with many different intentions including that of causing harm, embarrassment, disrepute and even fraud or forgery. Hence all hacking will not constitute forgery.

Even in case hacking results in forgery Section 66 of the Information Technology Act, 2000 specifically provides as under:

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

This section clearly specifies that a hacker will be penalised for his actions.

Secondly, Section 79 of the Information Technology Act, 2000 excludes the liability of a network service provider to any third party if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence, or contravention.

Given that the law has deemed it fit to specifically affix responsibility for hacking, on the hackers and not on any other party other than the hackers, the bankers should not be at any cost made party for hacking or for something that did not occur with its knowledge or instruction and where it had taken all reasonable and due care within its control.

Hence it may not be unreasonable for bankers to either limit their liability or specify and require via its bilateral agreements with the customers that losses on account of hacking are not its responsibilities.

Further I would like to submit that a bank does have protection against payment of a forged cheque albeit under certain circumstances. This problem is specifically dealt with in the Negotiable Instruments Act 1881 ("the Act"). Section 85 and 128 read with Section 10 of the said Act gives statutory protection to a paying banker in regard to loss by interloper fraud subject to the conditions that the payment must have been made in good faith and in due course. It has also been viewed that when an improper payment is made by the fact of the banker having been misled by contributory negligence or other fault on the part of the drawer, without which the forgery won't have taken place, then the bank can set up such negligence as a defence and secure the protection under Section 85 of the said Act. However, in order to do so, the bank must not be negligent. Thus, even with respect to the forged cheques, for occurrences beyond the control of the banker, a banker is exempted from any liability.

To strengthen my argument further, under the Information Technology Act, 2000, Section 42 clearly imposes the obligation on the subscriber to ensure that the private key is not compromised and the liability of the certifying authority for any compromise of the private key has been specifically excluded unless the subscriber informs the certifying authority of the same.

In the light all the above submissions and given the fact that law relating to the liability of banks on account of unauthorized transfer through hacking is still unsettled and evolving it would not be proper for the Working Group to conclude in its Report that the bank providing internet banking may not absolve itself from liability to the customers on account of unauthorized transfer through hacking especially in the light of the fact that this Report can be used, quoted and relied by any Person in any court of law as a persuasive authority.

C. To revert to the Report, in the same Paragraph 7.1 1.1, a similar conclusion has been reached with respect to denial of services. Denial of service can be either due to the circumstances beyond the control of the bank or due to non-compliance to the eligibility norms.

Very clearly, the bankers would be formulating transparent and pre-notified eligibility norms for availing of services by any person from it. Non-fulfilment of such eligibility norms would lead to denial of service by the bankers. Without probing into the actual eligibility norms, the intent of the same must be appreciated. These eligibility norms complement and supplement the know-your- customer philosophy and aids prevention as also combating money laundering, frauds, etc.

Reference drawn to the provisions of Section 43 of the Information Technology Act, is incorrect as the said provision states:

"if any person without the permission of the owner (the banker) or any other person who is in charge of a computer ... denies or causes denial of access to any person authorised to access any computer, computer system or computer network by any means, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

Clearly the section appreciates that the denial has not been caused by the owner, and in fact caused by a third party, and aims at ensuring compensation being payable by such third party to the party affected.

Upon raising queries with the relevant persons when the draft Information Technology Act was made available for comments, it was clarified that in case of damages beyond Rs one crore, the remedy for the person affected lies in the civil courts.

Clearly at no point in time, can the banker be made liable for denial of service due to circumstances beyond its control.

In this regard, I would like to draw your attention to Section 1693h of the U.S.Code which clearly provides exemptions to the liability of a financial institution in case of failure of the financial institution to make an electronic funds transfer, in accordance with the terms and conditions of an account, in the correct manner or in a timely manner when properly instructed if the financial institution shows by a preponderance of the evidence that its action or failure to act resulted from -

1. (1) an act of God or other circumstance beyond its control, that it exercised reasonable care to prevent such an occurrence, and that it exercised such diligence as the circumstances required; or
2. (2) a technical malfunction which was known to the consumer at the time he attempted to initiate an electronic fund transfer or, in the case of a preauthorized transfer, at the time such transfer should have occurred.

Conclusion:

In conclusion, as has been rightly noted by the Working Group that "the applicability of various existing laws and banking practices to e-banking is not tested and is still 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 establishment of the multidisciplinary high level standing committee to review the legal and technological requirements of e-banking on a continual basis and recommendations of appropriate measures as and when necessary, would really be a panacea for legal clarifications as and when they arise.

The key in such future and further deliberations would be to encourage banks towards innovation and where necessary or required evolve new practices and customs to complement the banking laws in force from time to time.

Annexure -2

List of Members of Working Group:

1. Shri S. R. Mittal, CGM-in-charge,
Department of Information Technology,
Reserve Bank of India,
Central Office,
Mumbai – 400 001 Chairman

2. Shri M. R. Srinivasan, Chief General Manager,
Department of Banking Supervison,
Reserve Bank of India,

Central Office,
Mumbai – 4-00 005 Member

3. Prof N. L. Sarda, Professor,
Indian Institute of Technology,
Powai, Mumbai, Member

4. Shri S. H. Bhojani, Dy.Managing Director,
ICICI Ltd, Mumbai Member
5. Shri Romesh Sobti, Chief Executive Officer,
ABN Amro Bank, Mumbai Member

6. Shri K. R. Ganapathy, Adviser,
Institute for Development and Research in Banking
Technology
Hyderabad Member

7. Shri Deepak Ghaisas, Chief Executive Officer,
i-flex solutions ltd. , Mumbai Member

8. Shri Ravi Nair, Vice President,
ICICI Bank Limited, Mumbai Member

9. Shri K. M. Shettigar, Dy. General Manager
State Bank of India,
Cental Office,
Mumbai – 400 021 Member
10. Shri M. P. Kothari, General Manager Member
Reserve Bank of India, Secretary
Central Office,
Mumbai – 400 005

Annexure-3

List of Members of Operational Group:

1. Shri G. P. Muniappan, Executive Director,
Reserve Bank of India,
Central Office,
Mumbai – 400001 Chairman

2. Shri A. Ghosh, CGM-in-charge,
Department of Banking Operations and
Development
Reserve Bank of India,
Central Office, Mumbai – 400 005 Member

3. Shri P. V. Subba Rao, Chief General Manager,
Department of Banking Operations and
Development
Reserve Bank of India,
Central Office, Mmumbai – 400 005 Member

4. Shri S. C. Gupta, Legal Adviser
Legal department,
Reserve Bank of India,
Central Office,
Mumbai – 400 001 Member

5. Shri V. S. Santhanam, Chief General Manager,
Department of Information Technology,
Reserve Bank of India,
Central Office,

Mumbai – 400 001 Member

6. Shri M. P. Kothari, General Manager,
Department of Banking Operations and Development
Reserve Bank of India, Member
Central Office, Mumbai – 400 005 Secretary

7. Shri Aditya Narain, Dy. General Manager,
Department of Banking Supervision,
Reserve Bank of India,
Central Office,
Mumbai – 400 005 Member

Annexure-4

References and Bibliography

1. The EDIFACT Standards – John Berge, NCC Blackwell, 1991
2. Authentication systems for Secure networks – Rolf Oppliger, Artech House, 1996 (www.artech-house.com, rolf.oppliger@esecurity.ch)
3. Introduction to PGP- Verisign (www.verisign.com)
4. Packet Magazine- Third Quarter 2000 Issue – CISCO systems (packet@cisco.com)
5. Understanding Public Key Infrastructure – RSA Security
6. A step by step guide for secure online commerce – Verisign (www.versign.com)
7. Architecture for Public-Key Infrastructure (APKI) - The Open Group (www.opengroup.org/public/pubs/catalog/g801.htm)
8. The Secure Sockets Layer Protocol – Netscape Communications Corporations (www.home.netscape.com/eng/ssl3/ssl-toc.htm)
9. The Risks of Key Recovery, Key Escrow & Trusted Third Party Encryption – Adhoc Group of Cryptographers & Computer Scientists (www.cdt.org/crypto)
10. Intelligence-Based Threat Assessments for Information Networks and Infrastructures -A White Paper - Kent Anderson Global Technology Research, Inc. (www.aracnet.com/~kea/Papers/threat_white_paper.shtml)
11. Security Extensions For HTML- Eric Rescorla, Allan M. Schiffman Terisa Systems, Inc. (www.ietf.org/proceedings/98aug/1-D/draft_ietf.wts.shtml)
12. The Secure Hypertext Transfer Protocol- Allan M. Schiffman Terisa Systems, Inc (ftp.isi.edu/in-notes/rfc2660.txt)
13. Maximum security – A hacker’s Guide to protecting Your Internet Site and Network –Anonymous (www.ods.com.ua/win/eng/security/Max_Security)
14. Federal Information Processing Standards Publication 191- Guideline for the analysis of local area network security (www.itl.nist.gov/fipspubs/fip191.htm)
15. Security Architecture for the Internet Protocol- Kent & Atkinson
16. The SSL Protocol Version 3.0 – Alan O. & Philip – Netscape & Paul C Kocher (www.fiddle.visc.vt.edu/courses/ecpc4984nad/files/rfc2401.txt)

17. Firewalls – IEEE Spectrum (www.spectrum.ieee.org)

18. CERT® Security Improvement Modules – CERT (www.cert.org/security_improvement)

19. Site Security Handbook - B. Fraser Editor SEI-CMU (www.csrc.nist.gov/secplcy/rfc1244.txt)

20. Security Issues in networks With Internet Access – Carl E Landwehr & David E Goldschlag (www.chacs.nrt.navy.mil/publcations/CHACS/1997/1997landwehr-PIEEE.pdf)

21. "Biometric techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable" - Dr. Despina Polemi , Report for the European commission DG XIII, 1997

22. NCSC-TG-009 - Computer Security Subsystems (www.radium.ncsc.mil/tpep/library/rainbow/ncsc-TG-009.html)

23. Electronic Banking Safety and Soundness Examination Procedures - Federal Deposit Insurance Corporation Division Of Supervision (www.fdic.gov/regulations)

24. The Information Technology Bill, 1999 (www.mit.gov.in/bill99.htm)

25. E Banking: Risks And Responses_Carol Sergeant Director, Banks & Buildings Societies Financial Services Authority –www.fsa.gov.uk

26. Hong Kong Monetary Authority – Guidelines – www.info.gov.hk/hkma

27. Australia – The Electronic Transactions Act – www.law.gov.au

28. Financial Services Regulatory Report – www.mayerbrown.com/legal/fin0696

29. Bank for International Settlements- Implications for Central Banks of the Development of Electronic Money, October 1996 (www.bis.org/publ/Disp01.pdf)

30. Committee on payment and Settlement Systems, Payment Systems in the Group of Ten Countries, Bank for International Settlements, December 1998

(www.bis.org/publ/cpss29.htm)

31. Committee on payment and Settlement Systems and the Group of Computer Experts, security of Electronic Money, bank for International Settlements, August 1996 (www.bis.org/publ/cpss18.htm)

32. Financial Action Task Force, FATF –VIII Money Laundering Typologies Exercise Public Report, February 1997 (www.oecd.org/fatf/Ar97_en.pdf)

33. Working group on EU Payments, Report to the Council of the European Monetary Institute on Prepaid Cards, European Monetary Institute, May 1994 (www.ecb.int, www.systemics.com/docs/papers/EU_prepaid_cards.htm)

34. Journal of Internet Banking and Commerce -- www.Arraydev.com/commerce/jibc

35. Arthur Anderson: Financial Services Research Paper-Issue No. 3 (www.arthurandersen.com)

36. JP Morgan securities Ltd. – Equity Research – Online Finance Europe

37. Enabling E-Commerce in India – www.giic.org

38. Business Models for Electronic Markets – CommerceNet (www.commerce.net)

39. E-Commerce: A white Paper – Keith Hazelton University of Wisconsin-Madison, 1998

40. Internet Banking Comptroller's Handbook, Comptroller of the Currency October 1999

Annexure-5

INTERNET BANKING GLOSSARY

Access Products - products that allow consumers to access traditional payment instruments electronically, generally from remote locations.

American National Standards Institute (ANSI) - a standard-setting organization; it is the U.S. representative to the International Standards Organization (ISO).

American Standard Code for Information Interchange (ASCII) - a standard code for representing characters and numbers that is used on most microcomputers, computer terminals, and printers.

Applet - a small application program that is designed to do a small, specific job.

Application - a computer program or set of programs that perform the processing of records for a specific function.

Asynchronous Transfer Mode (ATM) - method of transmitting bits of data one after another with a start bit and a stop bit to mark the beginning and end of each data unit.

Auditability - the degree to which transactions can be traced and audited through a system.

Authentication - the process of proving the claimed identity of an individual user, machine, software component or any other entity.

Authorization - the process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized different types of access or activity.

Bandwidth - the transmission capacity of a computer channel or communications line

Bastion Host - a system that has been hardened to resist attack, and which is installed on a network in such a way that it is expected to potentially come under attack. Bastion hosts are often components of firewalls, or may be “outside” web servers or public access systems.

Biometrics - a method of verifying an individual’s identity by analyzing a unique physical attribute.

Browser - a computer program that enables the user to retrieve information that has been made publicly available on the Internet; also permits multimedia (graphics) applications on the World Wide Web.

Chip - an electronic device consisting of circuit elements on a single silicon chip. The most complex circuits are microprocessors, which are single chips that contain the complete arithmetic and logic units of computers.

Chip Card - also known as an integrated circuit (IC) card. A card containing one or more computer chips or integrated circuits for identification, data storage or special-purpose processing used to validate personal identification numbers, authorize purchases, verify account balances and store personal records.

Client-Server Network - a method of allocating resources in a local area network so that computing power is distributed among computer workstations in the network but some shared resources are centralized in a file server.

Closed Network - a telecommunications network that is used for a specific purpose, such as a payment system, and to which access is restricted (also referred to as a private network).

Closed Stored Value System - a system in which value is issued and accepted by either a relatively small group of merchants, or in which the system is limited geographically (i.e., university programs and fare cards for mass transit systems).

Code - computer programs, written in machine language (object code) or programming language (source code).

Computer Emergency Response Team (CERT) - located at Carnegie-Mellon University, this incident response team offers advisories, which contain enormous amounts of useful, specific security information.

Cracker - a computer operator who breaks through a system's security. This can be legitimate activity, such as to test system security measures.

Cryptography - the principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form (i.e., scrambling a message).

Cyber Mall - a set of electronic or digital storefronts linked through a common web site.

Database Administrator (DBA) - the individual with authority to control the data base management system.

Data Encryption Standard (DES) - U.S. government standard for data encryption method published by the National Institute of Standards and Technology for the encryption of sensitive U.S. government data which does not fall under the category of national security related information. The DES uses a 64-bit key.

Data Integrity - the property that data meet with a priority expectation of quality.

Dedicated - assigned to only one function.

Dial-up - the ability of a remote user to access a system by using private or common carrier telephone lines.

Digital - referring to communications processors, techniques, and equipment where information is encoded as a binary “1” or “0”.

Digital Certification - a process to authenticate (or certify) a party’s digital signature; carried out by trusted third parties.

Digital Signatures - a mathematical encryption technique that associates a specific person with a given computer file and indicates that the file has not been altered since that person signed it; should not be confused with making an electronic representation of a written signature.

Distributed Transaction Processing - application processing that involves multiple users requiring concurrent access to a single shared resource.

Domain Name - an alphanumeric name for a web site that includes both the online address and online name.

Download - to transmit a file or program from a central computer to a smaller computer or a remote site.

Electronic Cash - the digital equivalent of dollars and cents (also referred to as digital cash).

Electronic Data Interchange (EDI) - the transfer of information between organizations in machine-readable form.

Electronic Document - the digital or computer equivalent of paper documents.

Electronic Money - monetary value measured in currency units stored in electronic form on an electronic device in the consumer’s possession. This electronic value can be purchased and held on the device until reduced through purchase or transfer.

Electronic Purse - a stored value device that can be used to make purchases from more than one vendor.

E-mail - messages people send to one another electronically from one computer to another.

Encryption (Cryptography) - the process of scrambling data by a device or encoding principle (mathematical algorithms) so that the data cannot be read without the proper codes for unscrambling the data.

End-to-end Encryption - the protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

Ethernet - a type of local area network originally developed by Xerox, communication takes place by means of radio frequency signals carried over coaxial cable.

File Transfer Protocol (FTP) - a standard way of transferring files from one computer to another on the Internet.

Firewall - a system or combination of hardware and software solutions that enforces a boundary between two or more networks.

Flowchart - a programming tool to graphically present a procedure by using symbols to designate the logic of how a problem is solved.

Gateway - a computer that performs protocol conversion between different types of networks or applications.

Graphical User Interface (GUI) - a way of communicating with a computer by manipulating icons (pictures) and windows with a mouse.

Groupware - software that allows a group of people to work on the same data through a network, by facilitating file sharing and other forms of communication.

Hacker - a computer operator who breaks into a computer without authorization, either for malicious reasons or just to prove it can be done.

Home Banking - banking services that allow a customer to interact with a financial institution from a remote location by using a telephone, television set, terminal, personal computer, or other device to access a telecommunication system which links to the institution’s computer center.

Home Page - a screen of information made available to users through the Internet or a private intranet; it is the “main page” that users are expected to read first in order to access the other pages that comprise the web site.

Host - also known as a host computer that is the primary or controlling computer in a computer network, generally involving data communications or a local area network.

Hypertext - electronic documents that present information that can be connected together in many different ways, instead of sequentially.

Hypertext Markup Language (HTML) - a set of codes that can be inserted into text files to indicate special typefaces, inserted images, and links to other hypertext documents.

Hypertext Transfer Protocol (HTTP) - a standard method of publishing information as hypertext in HTML format on the Internet.

Incident Response Team - a team of computer experts (internal or external) organized to protect an organization's data, systems, and other assets from attack by hackers, viruses, or other compromise.

Integrated Circuit Card (IC Card) - a plastic card in which one or more integrated circuits are embedded (also called a chip card).

Integrated Services Digital Network (ISDN) - a type of all-digital telephone service. ISDN lines provide a connection that can transmit digital data as well as voice, without a modem.

International Organization for Standardization/Open Systems Interconnection (ISO/OSI) – an international standard-setting organization. ANSI is the U.S. representative.

Internet - a worldwide network of computer networks (commonly referred to as the Information Superhighway).

Internet Service Provider (ISP) - an entity that provides access to the Internet and related services, generally for a fee.

Interoperability - the compatibility of distinct applications, networks, or systems.

Intranet - a private network that uses the infrastructure and standards of the Internet and World Wide Web, but is cordoned off from the public Internet through firewall barriers.

Issuer - in a stored value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it.

Key - A secret value or code used in an encrypting algorithm known by one or both of the communicating parties.

Local Area Network (LAN) - a network that connects several computers that are located nearby (in the same room or building), allowing them to share files and devices such as printers.

Lock and Key Protection System - a protection system that involves matching a key or password with a specific access requirement.

Logging - the storing of information about events that occurred on the firewall or network.

Magnetic Stripe - used on debit, credit, and identification cards to store encoded information read by card readers; less secure than computer chip cards.

Memory Card - an integrated circuit (IC) card capable of storing information only.

Middleware - facilitates the client/server connections over a network and allows client applications to access and update remote databases and mainframe files.

National Institute for Standards and Technology (NIST) – an established US agency, within the Department of Commerce to develop technical, management, physical and administrative standards and guidelines for the cost effective security and privacy of sensitive information in Federal computer systems. NIST issues the Federal Information Processing Standards (FIPS).

Navigation - moving through a complex system of menus or help files.

Network - a group of computers connected by cables or other means and using software that enables them to share equipment and exchange information. A system of software and hardware connected in a manner to support data transmission.

Node - any device, including servers and workstations, connected to a network. Also, the point where devices are connected.

Non-repudiable Transactions - transactions that cannot be denied after the fact.

Offline - equipment or devices that are not in direct communication with the central processor of a computer system, or connected only intermittently.

Online - equipment or devices that communicate with a computer network. Connections can be direct (as in a LAN using dedicated connections) or indirect (as in using the Internet).

Online Scrip - debit accounts on the Internet or other major computer network.

Online Service Providers (OSP) - closed network services that provide access to various computer sites or networks for a fee.

Open Network - a telecommunications network to which access is not restricted.

Open Stored Value System - a system that may be comprised of one or more electronic cash issuers of stored value that is accepted by multiple merchants or entities.

Operating System - a program that controls a computer and makes it possible for users to enter and run their own programs.

Packet Switching - a data transmission method that routes packets along the most efficient path and allows a communication channel to be shared by multiple connections.

Password - a unique word or string of characters that a programmer, computer operator, or user must supply to satisfy security requirements before gaining access to the system or data.

Password Cracker - a software program designed to conduct an automated brute force attack on the password security controls of an information system by "guessing" user passwords.

Password Sniffer - a software program that is illicitly inserted somewhere on a network to capture user passwords as they pass through the system.

Payment System - a financial system that establishes the means for transferring money between suppliers and users of funds, usually by exchanging debits or credits between financial institutions.

Personal Identification Number (PIN) - a sequence of digits used to verify the identity of a device holder.

Piggyback (Between-the-lines Entry) - a means of gaining unauthorized access to a system via another user's legitimate connection.

Point of Sale (POS) - a system of terminals that debits or charges a customer's account and credits or pays a merchant's account to effect payment for purchases at retail establishments.

Prepaid Card - a card on which value is stored, and for which the holder has paid the issuer in advance.

Privacy - in the context of a payment system, the property that no information which might permit determination of transactions may be collected without the consent of the counterparties involved.

Protocols - a standardized set of rules that define how computers communicate with each other.

Proximity Cards - cards that can be read from a short distance; mainly used for security and vehicle identification.

Public Key Cryptography - type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

Remote Payment - a payment carried out through the sending of payment orders or payment instruments.

Repudiation - the denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication.

Router - a computer system in a network that stores and forwards data packets between local area networks and wide area networks.

Scattering - the process of mixing the integrated circuit (IC) chip components so that they cannot be analyzed easily.

Search Engines - software programs that are capable of locating specified information or web sites on the Internet.

Secure Electronic Transaction (SET) - a set of standards jointly developed by Visa, MasterCard, and several technologies companies to facilitate secure credit card transactions over the Internet.

Secure Hypertext Transfer Protocol (SHTTP) - provides secure communication mechanisms between an HTTP client-server pair.

Secure Socket Layer (SSL) - a protocol for providing data security during transmission using data encryption, server authentication, and message integrity.

Server - a computer that provides services to another computer (the client).

Settlement - an act that discharges obligations with respect to funds or securities transfers between two or more parties.

Settlement system - a system used to facilitate the settlement of transfers of funds.

Simple Mail Transfer Protocol (SMTP) - a protocol used to transfer electronic mail between computers on the Internet.

Smart Card - a card with a computer chip embedded, on which financial, health, educational, and security information can be stored and processed.

Specification - documents that contain basic detailed data.

Spoofing - an attempt to gain access to a system by posing as an authorized user.

Standards - the rules under which analysts, programmers, operators, and other personnel in an information service organization work.

Stored Value Card - a card that stores prepaid value via magnetic stripe or computer chip.

Structured Query Language (SQL) - a query language used to manipulate large databases.

System Integrity - the quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation of the system.

System Specification - a baseline specification containing all the essential computer-based business system documentation. It is completed at the end of the Development Phase.

Systemic Risk - the risk that the failure of one participant in a funds transfer system, or in financial markets generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their obligations when due.

Systems Analysis - the performance, management, and documentation of the four phases of the life cycle of a business system: study, design, development, and operation.

Tamper-evident - the capacity of devices to show evidence of physical attack.

Tamper-proof - the proven capacity of devices to resist all attacks.

Tamper resistant - the capacity of devices to resist physical attack up to a certain point.

Telecommunications - data transmission between a computing system and remotely located devices via telephone lines, cable, or wireless technology.

Telnet - a protocol that permits users to access a remote terminal or another computer through a network; widely used on the Internet.

Threat Monitoring - the analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of system security.

Throughput - the total amount of useful work performed by a data processing system during a given period of time.

Topology - the arrangement of nodes usually forming a star, ring, tree, or bus pattern.

Traceability - the degree to which transactions can be traced to the originator or recipient (also referred to as auditability).

Transferability - in electronic money systems, the degree to which an electronic balance can be transferred between devices without interaction with a central authority.

Transmission Control Protocol/Internet Protocol (TCP/IP) - a standard format for transmitting data in packets from one computer to another, on the Internet and within other networks. TCP deals with the construction of the data packets while IP routes them from machine to machine.

Trap Door - a concealed and unauthorized entrance into a computer operating system, designed by the programmer.

Trojan Horse - a program that appears to perform a useful function and sometimes does so quite well but also includes an unadvertised feature, which is usually malicious in nature.

Truncation - dropping off part of a character string either to conserve space or because of limited space.

Trusted Computer System - a system that employs sufficient assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information.

Trusted Third Party - a reputable entity that authenticates one or more parties to an electronic transaction. The authentication process generally involves the issuance and administration of digital certificates.

Uniform Resource Locator or Universal Resource Locator (URL) - a way of specifying the location of available information on the Internet.

Upload - to transmit a file to a central computer from a smaller computer or a remote location.

Usenet - a set of many newsgroups distributed via the Internet.

Virtual Corporations - corporations that have no official physical site presence and are made up of diverse geographically dispersed or mobile employees.

Virus - a program with the ability to reproduce by modifying other programs to include a copy of itself. It may contain destructive code that can move into multiple programs, data files, or devices on a system and spread through multiple systems in a network.

Vulnerability - a weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security.

Web Page - a screen of information supporting the home page of a web site.

Web Site - the collection of an entity's home page and other proprietary pages located on the World Wide Web.

Wide Area Network (WAN) - a communications network that covers a wide geographic area, such as state or country, using high speed long distance lines or satellites provided by a common carrier.

World Wide Web (web, www) - a sub network of the Internet through which information is exchanged via text, graphics, audio, and video.

Worm - a program that scans a system or an entire network for available, unused space in which to run. Worms tend to tie up all computing resources in a system or on a network and effectively shut it down.