CHAPTER 6: RECOMMENDATIONS

6.1 Recommendations based on Survey Results

From the study of the perceptions of the respondents which indicate the prospects of internet banking in Gujarat, the researcher here identifies that parameters such as Effort Expectancy, Facilitating Conditions, Fulfillment, Service Quality & Trust does not exhibit the strong level of agreement among the respondents. Hence the internet banks providing different services to e-customers can apply following ways to increase the prospectiveness.

6.1.1 Recommendation 1: This study has shown that banking facilities which involve concentration on the component of speed, safety and risk have very strong relationship with the level of satisfaction exhibited by the internet banking users. It is the most correlated determinant of acceptance of internet banking. This indicates that internet banks themselves have major role in ensuring that more customers adopt internet banking. The more facilities the internet banks have in the terms of website, locations, security and risk and others, there will be more number of prospective users of internet banking services provided by the banks.

6.1.2 Recommendation 2: It is revealed from the study that Web Based Banking is very prospective and will become pervasive in the banks where the customers have strong preference towards web based banking. Not only that the customers who use the online banking for long time and find very few complaints regarding its usage will prefer such banks to be their internet banks in future also. Hence the internet bank service providers should concentrate more on building trust of the e-customers.

6.1.3 Recommendation 3: The consumers acceptance of the internet banking as the effective mechanism of transacting with the banks is highly dependent on the prior computer experience, usage, of the internet, awareness about the internet, banking services, knowledge of the manner in which the internet banking services are availed, support from the internet bank of the user. Not only that the training inputs provided by the banks to their employees in the terms of the technological changes which embrace the intense usage of internet also is responsible for ensuring that the more number of customers are converted into e-customers.

6.1.4 Recommendation 4: In future studies banks should consider more on bank and customer expectations. Therefore in factor regarding to Readiness the technology, designing value added benefits and considering the trustworthiness among
customers are more important. Also when considering the customer aspect it should focused more on accessibility, currency of service, meeting customer expectations, customer benefits and attractiveness of services as further improvements.

6.1.5 Recommendation 5: Since the competitiveness in the industry banks should focus more on innovative products and method of applying them on right time. Therefore through factor Strategy banks should improve their uniqueness, time benefits and technical aspects further. On customer aspect the factor Strategy should be more convenience, speedy access and user friendly on future products.

6.1.6 Recommendation 6: When future products are designed the banks have to consider the customer growth and the satisfaction. Thus considering the factor Approach banks should consider the future expansion of the customer base. On customer aspect the factor Approach should base on awareness, cost benefit, user friendly and accuracy of service when future decisions are made.

6.1.7 Recommendation 7: To meet the future competitiveness banks should consider on availability of facilities. Therefore in factor Desire banks should further maintain customer secrecy on new future products. On customer aspect the factor Desire should consider the auxiliary benefits, expectations and speedy service on future designed products.

6.1.8 Recommendation 8: Since the customer centric approach, banks are more focusing towards the accomplishing customer needs. For the factor Confidence banks shows positive attitudes towards the industrial benefits, responsiveness, reliability and continuity of service when future plans are designed. On customer point of view the factor Confidence should concentrate more on trustworthiness and features when adopting new methods.

6.1.9 Recommendation 9: Also in the future studies, it is recommended that banks should develop different customer retention programs for the Internet banking customers. For such instance, banks should implement positive and reward-based processes to prevent customers from switching to another bank by increasing the level of customer trust, the value and the interpersonal relationship with customers. Banks may build customer trust through public relations activities. If banks develop an image of a “good corporate citizen” through public relations and publicity then their organizational credibility and relational values may improve in the eyes of customers. Once such processes are implemented, customers switching to another bank will be more difficult and banks should find it easier to retain customers. As
more banking services are adopted, the banks should maintain high Switching Costs, which will make it more difficult for the Internet banking users to switch to another competitor.

6.1.10 **Recommendation 10:** Since the results of this study reveals five most salient criterias which indicate prospectiveness of internet banking future research should investigate the similarity between customers’ and service providers’ (banks) perceptions on Switching Costs in Indian banking context. This will help the financial industry to have a better understanding on both customers and banks similar perceptions regarding issues relevant to Switching Cost, Customer Satisfaction and Customer Retention. Also this study found that focusing customer satisfaction alone is not effective in building customer loyalty, future research may attempt to explore the “unexplored” constructs that customers would value most. The Internet customers will be more concerned on convenience issues such as easy accessibility, speed, use of technology or the service given by the bank staff. Given the importance of employee competence, future research should also examine the impact of employees’ behaviour that could affect Customer Satisfaction and Customer Retention.

**6.2 Recommendation based on Survey Results Vis-a- Vis Reserve Bank of India’s initiative on E-Commerce and M-Commerce**

The researcher also emphasize that for making Internet banking prospective in future not only recommendations derived from the survey results but recommendations based on the Reserve Banks of India’s Reports and data collected from the Internet and Mobile Banking Association must also be considered by all the internet banks. These recommendations are as follows.

**6.2.1 Recommendation relating to Security Standards to be followed by Banks**

6.2.1.1 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.

6.2.1.2 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.

6.2.1.3 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.

6.2.1.4 At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank’s system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. 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.

6.2.1.5 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.

6.2.1.6 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.

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

b. 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.

6.2.1.7 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.

6.2.1.8 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.

6.2.1.9 The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:

   a. Attempting to guess passwords using password-cracking tools.
   b. Search for back door traps in the programs.
   c. Attempt to overload the system using DdoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.
   d. Check if commonly known holes in the software, especially the browser and the e-mail software exist.
   e. The penetration testing may also be carried out by engaging outside experts (often called ‘Ethical Hackers’).

6.2.1.10 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.

6.2.1.11 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.

6.2.1.12 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.

6.2.1.13 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.

6.2.1.14 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.)

6.2.1.15 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)

6.2.1.16 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.

6.2.1.17 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.

6.2.2 Recommendation relating to Legal Issues to be followed by Banks

6.2.2.1 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.

6.2.2.2 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.

6.2.2.3 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.

6.2.2.4 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.

6.2.2.5 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. 20,000/-, for the purpose of deductible expenses. Since the primary intention of the above provision, which is to prevent tax evasion by ensuring transfer of funds through identified accounts, is also satisfied in case of electronic transfer of funds between accounts, such transfers should also be recognized under the above provision. The Income tax Act, 1961 should be amended suitably.

6.2.2.6 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.

6.2.2.7 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.

6.2.2.8 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.

6.2.2.9 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.

6.2.2.10 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.

6.2.2.11 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 the 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.

6.2.3 Recommendation relating to Regulatory and Supervisory Issues to be followed by Banks

6.2.3.1 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.

6.2.3.2 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.

6.2.3.3 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.

6.2.3.4 Record maintenance and their availability for inspection and audit is a major supervisory focus. RBI Guidelines on “Preservation and 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.

6.2.3.5 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.
6.2.3.6 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.