RECOMMENDATIONS ON POLICY & REGULATORY GUIDELINES FOR MOBILE BANKING IN INDIA

Dr. P. S. Aithal*.
*Srinivas Institute of Management Studies, Pandeshwar, Mangalore - 575 001, INDIA, psaithal@srinivasgroup.com

ABSTRACT

Mobile banking requires transparent and clear policy and regulations in order to provide privacy and safety on personal data and about the precision of the transmitted data and its potential misuse while carrying out mobile electronic financial transactions. The contracting parties, therefore, should be able to count upon the law to enforce the provisions of contracts that are concluded using (mobile) electronic devices, if required. Further, the customer should be able to trust the privacy of his personal sphere. A clearly defined regulatory framework is, hence, indispensable to boost consumer confidence and increase acceptance amongst broad sections of the society as well as to ensure smooth functioning of Mobile business. In this paper, we have discussed the various legal factors and regulatory challenges which affects secure electronic financial transactions, Existing Guidelines of Indian IT Act 2000, Recommendations based on our study on Policy and Regulatory Guidelines to Indian Government for Mobile Banking, Suggested Recommendations & Guidelines to Indian Banks while providing mobile banking Services to their customers, and certain guidelines to the customers while using mobile banking services.

Keywords: Mobile banking policy and regulatory guidelines, Indian IT Act 2000, Online banking.

Introduction:

Mobile banking requires transparent and clear policy and regulations in order to provide privacy and safety on personal data and about the precision of the transmitted data and its potential misuse while carrying out mobile electronic financial transactions. The contracting parties, therefore, should be able to count upon the law to enforce the provisions of contracts that are concluded using (mobile) electronic devices, if required. Further, the customer should be able to trust the privacy of his personal sphere. A clearly defined regulatory framework is, hence, indispensable to boost consumer confidence and increase acceptance amongst broad sections of the society as well as to ensure smooth functioning of Mobile business. The legal regulations imposed by the lawmaker, thus, intend to safeguard and balance both consumer- and business interests by setting rules and regulating the market as well as the usage of existing and emerging technologies. They impose the highest level of restrictions that govern legally carried-out transactions (Veijalainen et al., 2003). Regulations applicable to Mobile banking are generally guided by five principles (Heinemann et al., 2004) :

1. Legal enforceability of contracts

2. Consumer protection

3. Privacy of data (no unnecessary, unauthorized data collection)

4. Confidentiality of data (protecting authorized data from misuse)

5. Right of self-determination (to carry out or reject a communication)

In this paper, we have discussed the various legal factors and regulatory challenges which affects secure electronic financial transactions, Existing Guidelines of Indian IT Act 2000, Recommendations based on present study on Policy and Regulatory Guidelines to Indian Government for Mobile Banking, Suggested Recommendations & Guidelines to Indian Banks while providing mobile banking Services to their customers, and certain guidelines to the customers while using mobile banking services.

Policy on M-banking:

1. Legal Factors Affecting Secure electronic Financial Transactions :

(1) The Issue of 'Signature'

Although the growth of online transactions (particularly credit-based) has relied to some extent on trust, it has however, raised the issue of the legality of electronic transactions. Like e-consumers, legal authorities also equate digital signatures with manual signatures in the traditional contracting contexts. In reality, although the word 'signature' connotes letters and writing, and the term "digital signature" has been conceived in a generic and technology-neutral way, it has been argued that, to apply the term "signature" to what can be performed using (asymmetric) cryptography technology is "simply inappropriate and misleading" (Wind, 2001). But although digital signatures have acquired legal status, the legal definition of "digital signatures" is proving very difficult to map onto online security technology functions.

(2) Model Law on Electronic Signatures

In an attempt to bring additional legal certainty regarding the use of digital signatures, the United Nations Commission on International Trade Law (UNCITRAL) adopted a Model Law on Electronic Signatures in 2001. Based on Article 7 of the UNCITRAL Model Law on Electronic Commerce (1996), it inferred that subject to certain criteria of technical reliability, electronic signatures will be treated as equivalent to hand-written signatures. The Model Law thus adheres to a technology-neutral approach and avoids any bias toward the use of any specific technical product.

(3) The Indian Situation

(a) Current Legal Infrastructure

In any e-commerce transaction, it is important to guarantee that a valid contract has been entered between the parties especially since the contracts are paperless. Hence many developed countries have enacted legislation to this effect. However, in some nations, there is an absence of legislation on electronic transactions, and hence assessing the validity of electronic contracts and other electronic documents becomes complicated as existing legislation is inappropriate in dealing with online business transactions. This puts Indian businesses at a greater risk than businesses in developed countries when engaging in e-commerce transactions.

(b) Mobile Services Access and Cost

Although there is emphasis on security in the developed world, other major problems to the expansion of mobile financial transactions in the developing world are the lack of telecommunications and mobile phone connectivity.

(c) Increased Security

Further, since September 11, 2001, issues of authentication have now become extremely important. Many US web sites now only cater for US customers while former international customers, who were previously issued international visa cards, are debarred from engaging in online purchases. This has negative connotations for both local businesses and consumers to buy-in into global mobile banking. Consequently, there is a lack of confidence in digital signatures and a general reluctance to engage in mobile banking.

The Regulatory Challenges:

At the national level, the Indian government and the relevant regulatory agencies have strived to match the rapidly changing online banking environment with necessary regulations and institutional frameworks. Earlier efforts made to this effect included the enactment of the Failed Banks (Recovery of Debts) and Malpractices in Banks Decree No.18 of 1994, and the Money Laundering Decree of 1995. However, as noted above, poor enforcement procedure rendered these instruments very inactive. By the late 1990s, following record growth in Internet and computer usage in the country, almost all the regulations guiding the banking industry, including the *Banks and Other Institutions Act*, were lacking adequate provisions to accommodate the emerging trend. Not even a mention of electronic banking or any manner of its application was mentioned in any of those prevailing regulatory documents. The situation created a lot of gaps between the levels of regulatory tools and the advances in information technology. This at the same time made the banks vulnerable to all kinds of risks, including transaction, strategic, reputation and foreign exchange risks. This deficiency notwithstanding, it was not until 2003 when the maiden guidelines on electronic banking came into force. Despite its numerous technical specifications, the Guidelines have been widely criticized as not being enough to check the growing popularity of Internet banking against the backdrop of growing sophistication in technology related crimes and frauds. Closer examination of the contents of the Guidelines equally shows that the document fails to meet up with the four key areas where Internet banking may have regulatory impact – changing the traditional lines upon which existing regulatory structures are laid; handling concerns about existing public policy issues; changing the nature and scope of existing risks; and rebalancing regulatory rules and industry discretion. Part of the criticisms is that the recent guidelines that are capable of constraining the practice and development of mobile banking in India. One of such areas, for instance, is the requirement on electronic banking product development. While acknowledging that the existing regulations would apply wholly on electronic banking, The Guidelines also gives indications that the products/services can only be offered to residents of India with a verifiable address within the geographic boundary of the country; any person residing physically in the country as a citizen, under a resident permit or other legal residency designation under the Indian Immigration Act;. The Guidelines go further to indicate that the e-banking service should be offered in India only; and that where such a service is to be provided in foreign currency, it should be to only the holders of ordinary domiciliary accounts, and conform with all other foreign exchange regulations. On some other aspects, the Guidelines have also been criticized for not addressing adequately the critical issues concerning online security. It failed to explicitly recommend a standard that allows banks to examine potential threats that may already be in existence in each individual financial institution's current network. In addition to this array of criticisms, the workability of proper wireless technology framework is also queried amidst the poor state of basic information technological infrastructure in the country. This is essentially necessary since e-banking generally relies on the existence of adequate operational infrastructure like telecommunications and power to function effective. It is expected of the m-Banking Guidelines to provide procedures not only for banks' investment in Internet facilities, but also in promoting customers' access to such. Unfortunately, none of such is contained in the document.

Existing Guidelines of IT Act 2000:

1. Technology and Security Standards:

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 of IT act 2000).

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 of IT act 2000).

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 of IT act 2000).

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 of IT act 2000).

1.5 *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 of IT act 2000).

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

- Attempting to guess passwords using password-cracking tools.

- Search for back door traps in the programs.

- Attempt to overload the system using DdoS (Distributed Denial of Service) &DoS (Denial of Service) attacks.

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

- The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers') (Para 6.4.8 of IT act 2000).

1.7 *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 of IT act 2000).

1.8 *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 of IT act 2000)

1.9 *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 of IT act 2000)

1.10 *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 of IT act 2000).

2. Regulatory and Supervisory Issues

2.1 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 of IT act 2000).

2.2 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 of IT act 2000).

2.3 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 of IT act 2000).

2.4 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 of IT act 2000).

2.5 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 of IT act 2000).

2.6 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 of IT act 2000).

2.7. 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.

Recommendations:

Generally, credit card customers have complete legal protection for online purchases and aren't liable if the card is stolen or used without their authorization (Wolverton, 2002). However, the development of new technologies is rarely affected by law. Yet, as societal use of wireless technologies for online financial transactions becomes increasingly ubiquitous, the issue of the legality of these transactions arises since customers may even be at risk with the use of mobile technologies than they are with credit cards online. That is to say, in an online financial transaction, both parties usually want to be certain of the (a) origin, receipt and integrity of information they receive, and (b) authenticity and identity of each party. Thus, the enactment of laws recognizing the use of digital signatures is an exception to the above generality, given that m-banking needs "standards, regulations, and law to create an environment of certainty, trust and security" (Mann, 2000).

For developing countries to actively engage in mobile banking activities, it is necessary that an information infrastructure be initially developed and supported by the appropriate legislation. This can be achieved by promoting the development, expansion and operation of mobile telecommunication networks and services'. As it stands, mobile banking might take a reasonably long time to fully become of economic relevance in the country's banking practice. Even amidst the regulatory deficiencies identified above, the rising cases of online related frauds originating from different countries have made the online banking environment very complex. The banking industry in the country does not also at present enjoy that level of global integration that may allow for full benefits of mobile banking system. Even at home, the level of public confidence in the banks is not such that can guarantee effective customer patronage of mobile Banking services. Hence in addition to the cases of poor access to the requisite facilities, very few customers actually transact businesses through the wireless technology. This explains why the development of banks' web sites has not gone beyond information purposes. A situation where

banks would have to invest much on acquiring information technology software without attracting enough customer patronage necessary to justify the huge expenditure does not make for a progressive chance for rapid growth in mobile banking in India. With the deficiencies in the existing electronic banking guidelines, and the seemingly lack of proactive measures in other banking regulations in the country, the right environment for mobile banking remains presently not in existence.

5. 1. Recommended Policy and Regulatory Guidelines to Indian Government for Mobile Banking :

1. Improve system infrastructure environment for online mobile banking :

♦ Strengthen the mobile network infrastructure of the country to access the mobile banking services anywhere in the country.

♦ Improve the utility bill payment service system.

♦ Improve the settlement system for electronic online transactions.

♦ Improve the collaboration between mobile network service providers and financial service providers to use private network for online mobile financial transactions. This will improve the security of financial transaction compare to usage of open network like internet.

♦ Build-up transaction reporting and reconciliation services.

♦ Establish credit information registry and disseminating system. Credit information system can reduce the extent of asymmetric information by making a borrower's credit history available to potential lenders.

2. Create an enabling policy and regulatory environment for online mobile banking :

♦ Create an enabling policy to strengthen the protection of financial service providers rights and financial contracts by means of suitable laws and regulations.

♦ Improve the judiciary and contract enforcement system.

♦ Both private and public banks should have collaborative groups with mobile network providers in identifying risk management guidance and industry standards that can facilitate the development of online mobile banking within prudent risk parameters without unduly constraining its innovation.

3. Build up a comprehensive online security public policy framework :

The regulation of online mobile banking by government in terms of security is very important for public interest purpose.

♦ Both internet based transactions and transactions through private mobile network require their own security measures for which Government actions and controls are needed to set up a framework for digital signatures and to designate agencies or processes to authenticate public keys associated with transactions.

♦ Mobile communication industry and financial services sectors are crucial components of the online mobile financial services framework.

♦ The transaction through mobile network or internet implies that financial services are increasingly borderless and global. Hence mitigating electronic security risks requires unprecedented efforts to promote collective action within countries like inter-agency and public –private sector co-operation as well as across countries by market participants, regulators, and law enforcements.

♦ The security for online mobile financial transition is a risk management problem and proper regulations is required for balancing safety and privacy protection.

The historical role of governments in ensuring the orderly implementation of broad, general purpose technologies which are enabling and transformative in nature is well-known. One need only consider the extensive frameworks of legislation and ways of behaving that surround railroads, electricity, the telephone and the automobile. *For the mobile business to achieve its maximum social and political potential there will have to agreed upon and effective rules of the road, both nationally and globally.*

Government can play a critical role in developing and determining marketplace rules for the digital economy. Such rules can affect the foundation for the development of a high level of trust and confidence which is necessary for the successful operation of electronic marketplaces. Data protection and privacy, electronic signatures and authentication, spam and cyber-crime, including the threat of identity theft, have emerged as important areas where governments need to be either directly or indirectly involved in establishing such rules of the road. The Indian government has played a significant role in fostering the development of network infrastructure for today's information economy, as well as the ground rules that will be needed for an increasingly network-based economy. Such rules must not only adapt to new technologies, but also reflect the global, borderless nature of modern trade and commerce. Future economic growth, moreover, relies on a set of rules which are consistent and apply marketplace-wide. Accordingly, in order to maintain India’s competitive position internationally, the government has acted to make India a world leader in the adoption and use of electronic commerce, by creating a predictable and supportive environment that would ensure consumers and businesses feel comfortable, secure and confident in conducting commerce online. Traditional policy and regulatory instruments are usually limited in their application to national or sub-national jurisdictions. In the absence of complementary actions in other jurisdictions, however, domestic rule-making for marketplaces which are defined by the conduct of mobile-based business, will have limited effectiveness.

Thus, in order to meet national policy objectives effectively in areas such as data protection and privacy, electronic signatures, the regulation of spam and other offensive online content, and consumer protection measures, governments need to coordinate and align their domestic regimes with those in force outside their own jurisdictions, both bilaterally and on a multilateral basis. The public policy challenge for governments rests on their ability to redesign the ground rules for the conduct of international business - first, by adapting the traditional trade rules and disciplines developed through bodies such as the World Trade Organization (WTO) to the realities of a networked international economy dominated by m-business, and secondly, to harmonize the operation of domestic legal, policy and regulatory frameworks with international norms.

5. 2. Suggested Recommendation & Guidelines to Banks to Provide mobile banking Services :

(a) Recommendations :

The study revealed that “Proper Education & Training” and “Perceived Usefulness” were the most significant factors in encouraging online mobile banking adoption, and “External Environment” was the most significant factor to impede mobile banking adoption in India. It is essential for banks to facilitate encouragement and restrict impediment factors. Therefore, in addition to the direct “push” from banks (in respect of the encouragement factors), indirect persuasion should be carried out as a “pull” mechanism (in respect of the impediment factors).

“Push” strategies for encouragement factors :

Awareness of online mobile banking services is essential in the early adoption stages. As mobile banking services are still new in India, effective presentations using all forms of media advertising such as leaflets, brochures, web pages, etc., will be useful to introduce the services to a wider audience and educate potential customers about the benefits of online mobile banking. To access more potential adopters, information about mobile banking should be provided by bank tellers and bank assistants at branches. The information should include references to “time saving”, “convenience” at anywhere any time, “low costs”, and “information availability”. In addition, banks should design their web sites as effective delivery channels and offer information beyond banking services. Applying the notion of segmentation is also useful in this context; disseminating information through the right channel and the right mode of communication for different consumer segments is likely to increase each segment's probability to adopt technological innovations.

It is essential to provide a well-designed and user-friendly web site to attract potential adopters' attention. The customer should not be required to expend a lot of effort or time, or undergo too great a change in behavior, to adopt mobile banking services. Information and instructions for SMS banking or WAP banking should be provided in both local languages and English in order to make the adopter comfortable. Wide publicity underscoring the benefits and ease of use by demonstrating mobile banking services should be provided. This could be implemented by providing personal training at bank branches accompanied by good documentation and bank assistance. Regular surveying of customers' responses and opinions of the services should be conducted to ensure continuous improvement.

Reliability of access when needed is one of the key encouragement factors. Although this "reliability" partly depends on customers' mobile networks. Bank should also separate internal and external uses and give priority to external uses. While reliability is a key element from a customer's perspective, so is the security system. It must be enhanced continuously to guarantee integrity of online transactions as this will build customer confidence. Security provisions should be posted on banks' web sites clearly and understandably to create customer confidence and improve the trustworthiness reputation of banks. Security information should be provided in

non-technical terms, and be accompanied by standard security statements.

A perception of quality service will increase the bank's image for good services, accuracy and effectiveness. Failure of execution not only causes dissatisfaction and uncertainty to the customer but also makes the whole mobile banking process more complex and less comprehensible. Offering incentives in the form of accumulated points or little increased interest rate for deposits or providing loan for purchasing mobile phones at subsidized rate or having collaboration with mobile phone service providers to give free accessibility for online banking operations are other effective strategy to encourage online mobile banking adoption by Indian customers.

In summary, recommendations for "supplier push" strategies are as follows :

(1) Build customers' recognition of online mobile banking by

♦ emphasize the advantages of online mobile banking services, i.e. time saving, low cost services, convenience and information availability; and

♦ provide various types of information both financial and non-financial through proper education on this channel and training on usage.

(2) Attract customers to the mobile banking distribution channel :

♦ provide a well-designed and user-friendly mobile banking model;

♦ provide information in both Local and English languages;

♦ provide demonstrations in public places, e.g. bank branches, department stores, colleges etc.;

♦ provide both electronic and documentary demonstrations of online services; and

♦ regularly survey customers' responses to online mobile banking procedures and further develop the web site.

(3) Attract customers by ease of access:

♦ regularly monitor customers' access;

♦ implement traffic management systems for internal and external users;

♦ co-ordinate services with mobile communication service providers.

(4) Build customers' confidence:

♦ present the security used in both technical and non-technical terms;

♦ outline the procedure and information on how to cope with problems if they occur; and

♦ provide instructions on how to use online mobile banking services safely.

(5) Other strategies:

♦ offer incentives such as free service usage, frequent user benefits (like points), member rewards, etc.; and

♦ provide free access to banks' networks without any mobile network usage charges, etc.

"Pull" strategies for impediment factor :

Banks should develop online mobile banking diffusion strategies by adopting "pull" strategies. Increased diffusion will increase the number of mobile banking adopters since they are likely to come from the mobile phone users population. Furthermore, support from the government and the industry regulator will positively affect online mobile banking services by increasing the confidence of the adopters. Effective cooperation among banks has to be developed. The value of online mobile banking is increased by linking one activity with both within banks and with outside suppliers, channels and customers (Porter, 2001). Furthermore, banks should collaborate with mobile network service providers because it will enable banks to better control quality of services as well as enhance adopters' accessibility. In addition, a high quality mobile infrastructure should be provided since it is one of the primary requirements for mobile banking channel usage. In order to improve the authenticity and security of the financial transactions, banks should support to produce & purchase mobile phones with bio-metric identification technology.

Support from the government and industry regulator should be effective to increase the growth of online mobile banking services. The Indian government should be encouraged to initiate suitable steps to remove legal and regulatory barriers to mobile-business in general and mobile banking in particular. In addition to lobbying the Indian government, TROI and the RBI, banks should also proactively participate in improving mobile banking services in order to increase online banking. For example, IT 2000 laws should be promoted by the banks in order to reduce customers' perceptions of risks. Current co-operation has been for commercial purposes, rather than for mutual benefit of the industry. This may need the industry regulator, i.e. the RBI, to act as the central authority to improve the external environment.

In summary, recommendations for “market pull” strategies are as follows:

(1) Increase service value by collaboration:

♦ collaborate with mobile service providers;

♦ offer free mobile service access;

♦ expand banking service across banks; and

♦ increase linkages to suppliers and merchants.

(2) Be proactive:

♦ support the government to enact mobile business laws (IT 2000) ;

♦ work with the industrial regulator; and

♦ provide education on the uses of the mobile communication and online mobile banking.

Customer-targeting strategies

Banks should focus on people with high purchasing power as the first priority and attempt to shift them online. This requires extensive analyses of customers' needs and the provision of customized services that are of value to them.

In summary, recommendations for moderating factors are as follows:

(1) Target right customers:

♦ persuade people who use mobile phone, people have education, people in good positions and appropriate income to adopt the services.

(2) Provide value to customers:

♦ monitor the historical bank usage of customers to know their needs;

♦ provide customized services to customers;

♦ Provide incentives to the customers for usage of mobile banking distribution channel.

(b) Suggested Guidelines :

Users' main reason for using banking online is the speed of the service

♦ Allow users quick access to the information they want. Avoid delaying users by stringing them along over a series of pages with 'teaser' marketing strategies. Also be aware that the use of pop-up windows will disorientate and annoy some users.

♦ Graphics must add value to your site, particularly if they have long download times otherwise users may become frustrated with waiting.

♦ Keep the length of application forms to a minimum - users do not like to spend too long inputting information unless it is absolutely necessary. Ideally, only ask for the mandatory information, particularly for speculative insurance quotations.

Otherwise, mark critical fields.

♦ Ensure that progress through multiple screens of forms is made clear by providing orientation cues, e.g. 1of 4. Users are less likely to become frustrated and leave the site if they feel more in control.

Avoid the Use of Ambiguous Terminology

♦ Use the company logo as a link to the homepage, rather than duplicating the word 'home' especially in contexts where 'home' could relate to various things e.g. home insurance or home loans.

♦ Use key words that are clear to users. For example when looking for mortgages, many users did not associate this with "Borrowing" and therefore had difficulty finding the right page.

Provide interactive features that add value

♦ Offer interactive features on the site – make these relevant to the goals and concerns of your customers. Consider features such as loan and mortgage calculators, so that users can input their own details and see how the products on offer fit with their own unique circumstances.

Users must have confidence in your service

♦ Keep all product information up to date. Clearly indicate how recently the site has been updated – customers expect up-to-date information and their confidence in the site can be damaged by the presence of outdated links or references to obsolete information.

♦ Insurance and banking is perceived as a serious business and users do not visit these sites for entertainment. Features of sites such as "fun" areas, for example, may decrease users' confidence.

♦ Logos of your strategic partners can increase user confidence in your site if the company in question is well known and has a good reputation.

♦ Provide alternative points of contact like telephone numbers and address details – on-line customers may require a personal point of contact so that they can telephone, visit or write to your organization. This is particularly important for customers making significant financial decisions, such as choosing a mortgage.

♦ Avoid the use of small font sizes – visitors to your site can find it difficult to read and it can give the impression that there is too much information, or that they are being presented with the 'small print'.

Users expect to find more than an online leaflet

♦ Users have high expectations of online banking and insurance sites and therefore do not like to have to call up for further information. Ensure that your site provides as much functionality as possible to enable users to find all the information they require and complete their enquiries online.

Online Transactions

♦ Offer clear feedback on transactions that have been carried out on-line – users require confirmation that any details they have supplied have been received and acted on accordingly.

♦ Provide clear cues on the security measures taken on the site – customers are often concerned about the privacy of information they enter on-line, and may need reassurance before they proceed. Too much emphasis on security measures may alarm users, so strike the right balance.

Know your target audience

♦ Use a writing style that is appropriate for your target audience - potential customers can be alienated by a presentation style that they feel is targeted at a different group of people.

♦ Ensure graphics and pictures suit the branding and target audience for the site – users may find large images imposing, particularly images of faces. 'Young' faces can also alienate older customers, so consider the message conveyed by your graphics.

Provide incentives and bundled services through mobile banking

♦ Banks should provide incentives in the form of accumulated points or enhanced interest rates or preference in loans to the customers for usage of mobile banking services.

♦ Banks should promote online mobile banking through bundled services like providing insurance support, payment of utility bills, or providing customized services for interested customers in chosen area of customer interest.

5.3. Recommendation to the Customers :

Customers should make use of the new ubiquitous mobile banking distribution channel by knowing the advantages of such services. Customers should ignore fear on security of their banking account and fraudulent transactions. Customers should educate themselves to maintain the secrecy of their passwords and pin numbers to maintain secured mobile banking usage. The following are some recommendations to the customers based on present study :

Usage of Technology :

♦ Identify the communication technology and the device technology to be used/required for optimum financial information transformation with your bank.

♦ Study the online transaction instructions from the website/brochure of the bank to avoid confusion while performing on-move transactions.

♦ Identify additional technological requirement/up-gradation to enhance security & user authentication.

Know your banks Services :

♦ Identify the various services available and their advantages/limitations from the bank personnel.

♦ Pursue the bank personnel to give training for how to use various mobile banking services using your mobile phone.

♦ Identify the service charge and incentives offered by the banks for usage of various services through your mobile device.

♦ If your bank is not providing advanced mobile banking services like utility bill payment, micro payment for retailing at shops, find out from when it will be provided.

♦ Identify the bundled services provided by the bank through mobile banking as new distribution channel.

Know your banks & mobile service providers security :

♦ Security is an important aspect of online mobile banking transactions and the usage of this channel depends on how secured the transactions are with that particular bank. The usage of mobile banking services by the customers depends on how best security is provided by the banks and the network service providers.

♦ Customers have to opt for maximum security for their transactions by means of multiple level passwords/PIN and/or voice based or bio-metric based security levels. This provides fraud less transactions of their financial information.

♦ Customers should identify the technology used by both the banks and the mobile network service providers and compare it with National leaders in the industry. If the security part of the technology is convinced, then only the customers should try for mobile banking business.

Maintenance of better security :

♦ By keeping both mobile device and the password/PIN secretly, and using the services of private network providers, the customers can avoid any fraudulent transactions from their banking account.

♦ Using 3G technology enabled mobile devices, using network of such high tech service providers, and choosing the high secured server adopted banks, customers can get better security for long term without any risk.

Better models :

♦ The new models of online banking and payment with proper research and development on improving security will certainly improve customer's confidence on adoption of this new distribution channel.

♦ Financial payment both micro and macro level using mobile device will simplify and integrate the communication, entertainment and financial transactions so that customers can eliminate credit/debit cards.

♦ Ubiquitous financial payment through bank using mobile device allows customers to make efficient and timely decision on their investment and payments.

Confident in online services :

♦ Based on Govt. regulations and service providers' continuous technology up gradation, customers are getting confidence in online financial transaction using private networked mobile devices. Such success factors certainly improve the confidence in new users to use this new distribution channel.

♦ Since online financial services available 24 hours/365 days, and providing better convenience for customers to carry out their financial transactions, customers can enjoy the benefits of online services.

♦ By means of getting proper education and training on awareness & usage of mobile financial services available by the banks, users can definitely improve their confidence on such services.

Encashadvantages :

♦ The customers should encash the advantages of mobile financial services such as anytime, anywhere, any amount of time, low cost, and moderately secured.

♦ The customers can encash the opportunity of doing cashless business/purchases/transactions using mobile device.

♦ The advantages like ubiquity, personalization, reduced cost, flexibility, increased comfort, time saving, convenience, and better cash management opportunity makes the mobile banking service as a killer application.

Conclusion:

A suitable policy & regulatory guidelines are suggested to the financial institutions to strengthen the mobile business framework in financial sector in India. The paper includes the summery of existing policy on e-banking with legal factors affecting secure electronic financial transactions, current legal infrastructure in India, mobile services access & cost, increased security and regulatory challenges. The existing guidelines of Indian IT act 2000 in the area of technology & security standards, legal issues, regulatory and supervisory issues are discussed. Finally recommendations have been made on regulatory guidelines to Indian Government for mobile banking. Guidelines are also suggested to Indian banks to provide mobile banking services and customers to encash the opportunity.

REFERENCES

1. Abel EbehEzeoha, (2005) Regulating Internet Banking In Nigeria : Problems and Challenges – Part 1 Journal of Internet Banking and Commerce, vol. 10, no.3.
2. Adepoju S. A., Babalola G. A., Onyeabor G. A.,(2011), Customers' Adoption and Usage of the Internet Banking and Other Web Services in Banking, International Journal of Management & Business studies, vol. 1, Issue 4, pp. 48 - 51.
3. Heinemann A., Ranke J., Straub T., (2004) :ZurrechtsverträglichenTechnikgestaltunganhandeiner M-Commerce-Anwendung, online available: http://nibbler.tk.informatik. tudarmstadt. de/publications/2004/ mc4.pdf, downloaded on 11.01.2005.
4. IT Act 2000, online available: downloaded from http://www.dot.gov.in/act-rules/information-technology-act-2000 on 25/12/2008.
5. Mann, et al. (2000), Global Electronic Commerce: A Policy Primer. Institute for International Economics, USA, July 18, 2000.
6. Porter, M. (2001) "Strategy and the Internet, "Harvard Business Review, March 2001, pp. 62-78.
7. Richard M. Escalante,Socio-Legal Issues Affecting the Use of Digital Signatures for Secure E-commerce Transactions: A Caribbean Perspective, Downloaded from http://www.arraydev.com/commerce/JIBC/0403-05.htm
8. Veijalainen J, Yamakawa P, Markkula J, et al. (2003) : On Requirements for Mobile Commerce, online available: http://www.mbusiness 2003.org/resources/Papers/01009.doc, 10.12.2004.
9. Wind, Y., (2001), "The Challenge of Customization in Financial Services," Communications of the ACM, Vol. 44, No. 5, pp. 39-44.
10. Wolverton, T. (2002). Wells Fargo to shutter mobile service. Retrieved from http://news.cnet.com/Wells-Fargo-to-shutter-mobile-service/2100-1017_3-954592.html on 25/12/2008.