CHAPTER - 4
CHALLENGES OF MOBILE BANKING

After having discussed services provided by mobile banking in the previous chapter, this chapter attempts to describe the challenges of mobile banking. The chapter is presented under the following heads:-

4.1 Advantages of Mobile Banking
4.2 Challenges of Mobile Banking
4.3 Disadvantages of Mobile Banking
4.4 Financial Inclusion through Mobile Banking

4.1 ADVANTAGES OF MOBILE BANKING

Internet Banking helped give the customer's anytime access to their banks. Customer's could check out their account details, get their bank statements, perform transactions like transferring money to other accounts and pay their bills sitting in the comfort of their homes and offices. However the biggest limitation of Internet banking is the requirement of a PC with an Internet connection, not a big obstacle if we look at the US and the European countries, but definitely a big barrier if we consider most of the developing countries of Asia like China and India. Mobile banking addresses this fundamental limitation of Internet Banking, as it reduces the customer requirement to just a mobile phone. Mobile banking is a technology that allows you to access your bank account from a mobile device, usually a cell phone. There are several benefits to this technology, particularly for activity notification and account management while traveling.

Mobile usage has seen an explosive growth in most of the Asian economies like India, China and Korea. In fact Korea boasts about a 70% mobile penetration rate and with its tech-savvy populace has seen one of the most aggressive rollouts of mobile banking services. Still, the main reason that Mobile Banking scores over Internet Banking is that it enables ‘Anywhere Banking'. Customers now don't need access to a computer terminal to access their banks, they can now do so on the go – when they are waiting for their bus to work, when
they are traveling or when they are waiting for their orders to come through in a restaurant.

Mobile banking has become increasingly popular over the years. Banks offer mobile banking to their clients as a convenience, but also because mobile banking saves these institutions considerable money. Here are some characteristic/features to consider with mobile banking:

4.1.1 Expanding Distribution and Coverage Models:

Mobile banking gives banks the potential to expand beyond their geographical footprint as well as ability to cross-sell and up-sell products to existing customers. Banks that harness these additional mobile financial services capabilities can see a profound impact on the nature of the banking relationship.

4.1.2 Monetizing the Value of Customer Analytics:

Unlike supermarkets, department stores, and other businesses that see only one dimension of consumers’ spending habits, banks have a broader view of what their customers buy and where they like to shop. This puts banks in a specific position to develop a new line of business focused on bundling data analytics for retailers and other entities vying for customer intelligence — while maintaining the privacy of individual customers’ information. Merchants could employ such aggregated information to target customers more effectively than they might through other means. In addition, banks could use this knowledge of their core customers to strengthen their own abilities to acquire new customers, cross-sell existing customers, improve decisioning capabilities, and provide better customer service — resulting in significant value streams for banks.

4.1.3 Delivering Greater Real-time Access to Products and Services:

Mobile banking could provide bank customers with the ability to compare options at time and place of purchase. At the same time, banks could offer these shoppers complementary services, such as financing or leasing options, insurance quotes (through partnerships), and more.
4.1.4 Offering Discounts and Purchasing Incentives to Bank Customers:

By establishing relationships with manufacturers and retailers that could offer bank customers discounts while they research product options at the point of sale, banks can position their mobile channel as something more than just a convenient way to pay.

4.1.5 Conducting Targeted Marketing Campaigns:

Similarly, banks could conduct a variety of targeted marketing campaigns to customers who use mobile banking. For example, banks could pinpoint shoppers’ physical locations to make relevant offers to their customers, such as offering them temporary line increases. In addition, banks could leverage the mobile banking interface as a real-time, tailored advertising engine by using behavioral analytics they compile to develop campaigns tailored to customers’ shopping preferences. Additionally, banks might be able to offer their customers “smart” coupons while customers are in stores shopping for a flat-screen television or digital camera. The coupons would come from alliances banks form with the products’ manufacturers and/or retailers — and banks would receive a fee for each coupon used.

4.1.6 Mobile Banking Specific Services:

Mobile Commerce makes it possible to offer services specific to a given context (e.g. time of the day, location and the interests of the user). Such services offer new opportunities for personalized push-marketing in close proximity to the vendor thereby increasing the probability of sale. It enhances brand presence and thus encourages consumers to remain loyal to brands they are acquainted with.

4.1.7 Time-critical Situations:

The ubiquity and immediacy of Mobile Commerce allows users to perform urgent tasks in an efficient manner, e.g. fast reaction to stock market developments irrespective of current geographic location.

4.1.8 Spontaneous Decisions and Needs:

Spontaneous needs are not externally triggered and generally involve decisions that do not require a very careful consideration, e.g. decisions involving
small amounts of money. Users may be provided with access to entertainment content, e.g. horoscope or sport news while on the move and with free time on the hand.

4.1.9 Efficiency Increase:

Mobile Commerce may help increase the productivity of the workforce by increasing the efficiency of their daily routines. Time-pressured consumers (employees) can use ‘dead spots (an area where activity lags)’ in the day, e.g. during the daily travel to and from workplace, more effectively. This can be utilised, e.g. to check e-mails, get current news, order products and carry out bank transactions.

4.1.10 Location-centric:

Not only is mobile phone in all places, Global Positioning System (GPS) may be created to recognize phone and tries to personalize based on existing services. Identifying the location of Internet users, provides a special advantage for mobile commerce over wired e-commerce. Using this technology, the mobile commerce providers will enable to receive and send information to a particular place.

4.1.11 Convenience:

Other people are not limited by time or space, access tom electronic activities. For example, people who are stuck in traffic or waiting in the queue Will be enable to buy their favorite Internet-based activities or managing their daily transactions through mobile commerce applications .Consumers can know a special comfort that can improve their quality of life. By making services more comfortable, the customer will be more loyal. As a result, Communication facilities with mobile commerce applications to provide a comfortable.

4.1.12 Customization:

Mobile phone is much higher influence than personal computers. Therefore, mobile commerce producers to design more creative and more customized lifestyle tool. For example, using demographic data collected by wireless service providers, and information on the current location of the mobile
users can do more targeted advertising. Advertising messages can be customized based on the information provided through consultation with the user's initial or previous users' shopping habits.

4.1.13 Identify Ability:

Mobile phone provides to support the secure mobile phone transactions where personal computers are almost unknown (no name). One person always uses mobile devices and it is ideal for Personal-based target marketing. Through the technology of Global Positioning System (GPS), service providers can recognize a user carefully. Personalize opportunity to deliver messages to different parts of space and time through sound and look.

4.2 CHALLENGES IN MOBILE BANKING

4.2.1 Handset Operability:

There are a large number of different mobile phone devices and it is a big challenge for banks to offer a mobile banking solution on any type of device. Some of these devices support Java and others support SIM Application Toolkit, a WAP browser, or only SMS. Initial interoperability issues however have been localized, with countries like India using portals like "R-World" to enable the limitations of low end java based phones, while focus on areas such as South Africa have defaulted to the USSD as a basis of communication achievable with any phone. The desire for interoperability is largely dependent on the banks themselves, where installed applications (Java based or native) provide better security, are easier to use and allow development of more complex capabilities similar to those of internet banking while SMS can provide the basics but becomes difficult to operate with more complex transactions.

There is a myth that there is a challenge of interoperability between mobile banking applications due to perceived lack of common technology standards for mobile banking. In practice it is too early in the service lifecycle for interoperability to be addressed within an individual country, as very few countries have more than one mobile banking service provider. In practice, banking interfaces are well defined and money movements between banks follow
the ISO-8583 standard. As mobile banking matures, money movements between service providers will naturally adopt the same standards as in the banking world. Every device does not have the facility for mobile banking. Some banks even do not provide users the facility of mobile banking. Of the banks that allow mobile banking, some banks require users to use a custom application for mobile banking that is available only on a few phones like Apple’s iPhone and Blackberry phones. Software from third parties for mobile banking is not supported. If a user does not have a smart phone, mobile banking is limited. You can check your bank account balance through text messages, but advanced features like account transfers are not available on regular phones.

4.2.2 Security:

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments.

WAP is used for communication between devices like digital mobile phones, internet, PDA etc. Through WAP customer can realize more functionality of internet banking. Encryption process is currently used for secure data transmission between bank and users but the problem is that this encryption process is not good enough for the protection of sensitive data between bank and customer. The reason is that security methods require more powerful computing and high storage capacity. If we take internet banking it is realized that there are powerful computer systems and well defined complex encryption process to ensure the security. Mobile device have low computational capacity and hence we are unable to apply complex cryptographic system. Due to advancement in technology, it is now necessary to provide end-to-end security. It means that if user uses his/her mobile device for mobile banking then the data transacted are secure at the bank end and not at the user end, thus leaving the data vulnerable to attacks. It was noted that it is difficult to provide end to end security through WAP. The reason is that the data is not encrypted at gateway during the switching of protocol process, which leads to security concern for mobile
banking in WAP. In China, mobile communication group introduced the —China Mobile Communication and Information Resources station entities and Internet short Message Gateway Interface Protocol. It was noted that security is the susceptibility in WAP and that it is safe for the information to be delivered from the gateway to end user but due to accessibility of information for short time on gateway it may be possible for the attacker to access the information. It is identified that users are not usually satisfied from mobile commerce over WAP. The reason is that, problems occur for reasons like low speed, unreliable connection, and high cost. A research on adaption of WAP services especially for mobile commerce market is in progress in countries like Hong Kong, China, Taiwan i.e. China economic region. In South Africa, there are two technologies used for mobile banking namely WAP and WIG (Wireless Internet Gateway) WIG is a short message service. For South Africa, security and cost are the most important issues in providing the service.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network:

- Physical part of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
- Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application.
- Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions.
- User ID / Password authentication of bank's customer.
- Encryption of the data being transmitted over the air.
- Encryption of the data that will be stored in device for later / off-line analysis by the customer.
- Mobile Malware - Trojans, viruses and rootkits migrating from traditional online banking and designed specifically for the mobile marketplace.
Researchers see an increase in mobile malware development - in pace with market growth.

- Third-Party Apps - Consumers love their smart phone and tablet applications, but often these apps come from third parties with questionable security practices. Or worse, the apps are created by fraudsters and loaded with malware.

- Unsecured Wi-Fi - The unsecured wireless network is a toll-free highway for fraudsters to gain access to mobile devices, either to seize control of or gain access to account information.

- User Behavior - Consumers are prone to download third-party apps, use unsecured wireless networks, open and click links in SMS text messages and e-mails, and lose their mobile devices. Mobile-use behavior is creating a suite of vulnerabilities, and fraudsters are eager to take advantage.

- As default data format for SMS is plaintext. Currently end to end encryption is not available. The only encryption involved at base transceiver station and SMS bank server during transmission. The encryption algorithm used is A5 which is proven to be defenseless. The most dangerous attack in SMS banking is spoofing attack where attacker can send messages on network by manipulating sender’s number. Due to spoofing attack, most of the organizations are not adopting mobile banking through SMS.

- There are more than fifty thousand different types of computer viruses, internet malicious program and Trojans. Software like Trojan horses can easily take up password on the web browser or any cached information on operating system. Malicious codes are written for remote communication. Zeus Trojan targeted mobile bank users. Zitmo has been used by attackers to defect SMS banking. Zeus is commonly used to steal mobile transaction authentication number or password.4
4.2.3 Economic Challenges in Adoption of Mobile Banking:

The rural population in India is spread across 600,000 villages, each with a low transaction value. Profitability can only be achieved by large volumes, requiring significant initiative from financial institutions. Unlike the very successful M-PESA of South Africa, whose model has been very successful due to the lack of alternative payments in South Africa, India does possess some infrastructure in the forms of postal payments, reasonable transport and local governments. Therefore, any mobile banking must be inexpensive enough to be attractive for the end-customer over existing methods.

4.2.4 Regulatory Challenges in Adoption of Mobile Banking:

Although the RBI is supportive of mobile banking in India, there are many regulations that are being put into place:

- Restricted to Financial Institutions: The guidelines state that only existing financial institutions and banks are allowed to offer mobile banking. Although the guidelines cover Microfinance Institutions (MFIs), significant economies of scale cannot be achieved by these due to existing large fixed costs. For a very inexpensive solution, it would have been more effective to allow non-profit organizations or evangelical organizations to build their own MFI without being encumbered by large existing infrastructure.

- Rupee Transactions: All transactions must be done only in India’s national currency, the rupee. While this may not be a threat in the beginning, this may pose a constraint for interoperability between Indian mobile payments and the world. Also, it excludes providers from the lucrative remittance market in India and limits areas from which mobile operators can be profitable.

- Existing Account Holders: The guidelines also state that only those having a valid bank account would be allowed mobile banking. This limits the full potential of mobile banking to extend micro-credit and bring banking to the large number of unbanked customers in India.
4.2.5 Demographic Challenges:

India has 18 official languages which are spoken across the country. The state governments also are dictated to correspond in their regional language for official purposes. Additionally, two-thirds of the population in India is illiterate, creating difficulties in deployment of mobile banking solutions. For a pan-Indian mobile banking solution, this will be cumbersome to overcome.

4.2.6 Authentication Risks and Issues:

One of the authentication method used in mobile banking is the login method. However PINS authentication method is an old method and many security issues such as password and id theft were discovered in this method. In such cases, the secret may be revealed and this results in customer’s distrust on the security service company. Bank follows some security mechanisms in mobile banking. While the customers and the banks are bound to each other. This security mechanism is done by identifying the customer’s phone number, SIM card number, pin number etc. Customer likes to use the mobile banking technology because of its mobility as they can access the bank anywhere and in any situation. They can transfer their money from one account to another account faster in a user-friendly environment. And also they can check the current status of their account. But all customers of the bank are not ready to use this service because of some security issues. They are not ready to adopt the mobile banking systems as it brings inconvenience to the users assuming that it cannot prevent direct or indirect attacks. The security mechanism adopted by the banks face many security issues like being attacked by unauthorized users which is of highest priority in terms of security. If the device gets stolen then the hackers or unauthorized persons may find the password from the log files or saved draft files. Many customers save their password in their mobile or they may keep the password under auto fill settings of the form, this loophole can be easily used by the unauthorized person. Uneducated people are less aware of these issues and thus leading to loss of trust by customers.
4.2.7 Reliability:

Another challenge for the banks is to scale-up the mobile banking infrastructure to handle exponential growth of the customer base. With mobile banking, the customer may be sitting in any part of the world (true anytime, anywhere banking) and hence banks need to ensure that the systems are up and running in a true 24 x 7 fashion. As customers will find mobile banking more and more useful, their expectations from the solution will increase. Banks unable to meet the performance and reliability expectations may lose customer confidence. There are systems such as Mobile Transaction Platform which allow quick and secure mobile enabling of various banking services. Recently in India there has been a phenomenal growth in the use of Mobile Banking applications, with leading banks adopting Mobile Transaction Platform and the Central Bank publishing guidelines for mobile banking operations.

4.2.8 Application Distribution:

Application distribution Due to the nature of the connectivity between bank and its customers, it would be impractical to expect customers to regularly visit banks or connect to a web site for regular upgrade of their mobile banking application. It will be expected that the mobile application itself check the upgrades and updates.

4.3 DISADVANTAGES OF MOBILE BANKING

- Every device does not have the facility for mobile banking. Some banks even do not provide users the facility of mobile banking. Of the banks that allow mobile banking, some banks require users to use a custom application for mobile banking that is available only on a few phones like Apple’s iPhone and Blackberry phones. Software from third parties for mobile banking is not supported. If a user does not have a smart phone, mobile banking is limited. You can check your bank account balance through text messages, but advanced features like account transfers are not available on regular phones.
• If you have a compatible device then the cost of mobile banking might not matter much to you, but if you have to pay for the data and the texting fee then it might cost you some amount of money. Some banks will charge users an extra fee for the service and also users have to pay a fee for the software too. If you use mobile banking regularly then all the extra charges might make a significant amount that you will have to pay.

• Security experts opine that mobile banking is more secure than computer banking since there are very few viruses, Trojans etc on mobile than on computer. However, it does not mean that mobile banking does not have any security threats. Users of mobile banking can be prone to scam similar to phishing termed “smishing”. It happens when a user receives a fake message asking their bank account details from hackers who disguise as people from financial institutes. Many people were caught with this trick and lost their money because of this scam.

• The loss of a person’s mobile device often means that criminals can gain access to your mobile banking PIN and other sensitive information.

• Modern mobile devices like Smartphone and tablets are better suited for mobile banking than old models of mobile phones and devices.

• Regular users of mobile banking over time can accumulate significant charges from their banks.

• Even though there are 1.5 billion computers on the Internet and 4.5 billion people using mobile phones, there’s currently no significant operating system supporting the mobile space. “Hackers want to do the least amount of work for the biggest gain.”

• Most mobile banking apps need an internet connection to be able to operate, so if you live in a rural area or experience problems with your internet connection, then you won’t be able to access your account. The same applies if your mobile phone runs out of battery.

• Many phones aren’t yet compatible with anti-virus software. Most cell phones don’t come standard with anti-virus protection even if they have
the capacity to browse the internet. Some phones aren’t even compatible with the anti-virus software available and there are known cases in which people were unable to put anti-virus software registered to them on corporate cell phones. Although identity thieves are still a few steps behind when it comes to learning to implement some of their most successful computer tricks (phishing, spamming, spreading viruses, account hacking, etc…) on a cell phone level, experts agree that is only a matter of time and people shouldn’t assume that anti-virus software isn’t necessary for cell phones.

- Some banks don’t offer the same level of protection for cell phone banking that they do for online or in person transactions. Because the risks are still generally unknown some banks have been slow to make promises about what will or will not be covered when you use cell phone banking.

4.4 FINANCIAL INCLUSION THROUGH MOBILE BANKING

There is increased emphasis on financial inclusion from the Government, regulators, banks, NGOs, and individuals. Proponents of development finance like Md. Yunus are going to the extent of making it as a fundamental right of an individual. But, there is demand as well as supply side constraints to it. A large section of the society is deprived of financial services like credit, loan, insurance, financial education, remittances, pension etc. So does it mean that the poor are not availing the financial services? The answer to it is no. They have got their own mechanism to do so, and they do it in multiple ways involving informal sources (Collins et al, 2009). Here, informal methods serve the purpose, but it is much more costly and has various ill effects. In this situation mobile banking seems to a feasible solution. It has got benefits for multiple stakeholders. At the macro level use of mobile banking will increase the flow of money, spread entrepreneurship, and increase Gross Domestic Product. At the same time there are limitations or dangers of mobile banking at macro level. It could lead to increased instances of money laundering and may be in criminal activities.
Whereas, at micro level it will benefit the organization as well as consumers in terms of addressing constraints being faced by them.

With more than one and half lakhs of branches, post offices are really hard to ignore by Banks when it comes to fulfilling the mandate of financial inclusion. It also makes economic sense, because it saves the cost of setting up branches in the respective area as well as provides some localized knowledge inbuilt in the system. Localized knowledge will help in mitigating the behavioral issues in adoption of mobile banking. In order to facilitate financial inclusion we propose a tripartite arrangement between banks, post office, and mobile operators/business correspondence (BC) as under.

**Figure 4.1: Tripartite Arrangement for Financial Inclusion**

![Tripartite Arrangement for Financial Inclusion](http://ssrn.com/abstract=2485777)

The arrangement will be such that post offices will be divided on regional basis and bidding would be done by interested banks for that particular region. One might argue that this responsibility should be given to Lead Banks of respective region as they are already working on similar lines and have established their foot hold in their respective areas. The lead banks are based on social responsibility assigned to the banks having maximum network in the area under consideration. Our idea is to make this arrangement on commercial basis,
and linking it with social responsibility might dilute it. Moreover the impact of Lead Bank Scheme is not so encouraging. A Report of the High Level Committee to Review Lead Bank Scheme has identified several weaknesses in the system which has adversely affected its working. In view of this, we propose to have a separate arrangement based on commercial interest. Since post offices have reach with readymade infrastructure, it will save a lot of cost for banks and provide a brick and mortar retail outlet to serve the customers. After getting the bid of a particular region, the banks concerned would have one employee working in the post office. The bank would also provide training to existing post office employees and appraise them about the working of financial system especially focused on financial inclusion. To supplement it, mobile banking system with the help of mobile operators working in the same area or some NBFCs would be integrated. 5
REFERENCES:


