International Indexed, Refereed Research Journal, ISSN-2250-2629(Print), E-ISSN 2320-5466, Issue-3, Vol-I, March-2013

Research Paper - Law

Security Measures for Mobile Banking

*** Dr. Sunita Arya**

*** Assistant, Professor ,Shri Vaishnav Institute of Law, Indore M.P.**

A B S T R A C T

Mobile banking is one of the most significant technological innovations of the 21st century. Time saving is most important in today's busy world. It allows customers of a particular bank to do their daily banking on their smart cell. This is very useful hi-tech phenomenon which not only helps to customers but also to the banks now it has become a buzz in the world of banking. Consultative Group to Assist the Poorest (CGAP) and Microsoft Research India (MSRI) are collaborating on joint research to better understand the needs of people who have low levels of literacy when it comes to technology. This means to know how to design something that would be of use to an illiterate person. In addition to the focal research on User Interface design, the MSRI-CGAP collaboration will also involve joint explorations in understanding the social and economic context and impact of mobile-banking on poor households. Mobile banking is a system that allows customers of a financial institution to conduct a number of financial transactions through a mobile device such as a mobile phone or personal digital assistant.

Keywords: ***Financial Transactions, Digital Assistant Fraudulent Developers, Personal Identification Number, Ensure Confidentiality***

Introduction:

Mobile banking differs from mobile payments, which involve the use of a mobile device to pay for goods or services either at the point of sale or remotely[1], analogously to the use of a debit or credit card to affect an electronic fund transfer at point of sale (EFTPOS) payment. The earliest mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart cells with Wireless Application Protocol (WAP) support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers.[2]

Mobile banking has until recently most often been performed via SMS or the mobile web. Apple's initial success with I-Phone and the rapid growth of phones based on Google's Android (operating system) have led to increasing use of special client programs, called apps, downloaded to the mobile device. With that said advancements in web technologies such as HTML5, CSS3 and JavaScript have seen more banks launching mobile web based services to complement native applications. A recent study (May 2012) by Mapa Research suggests that over a third of banks[3] have mobile device detection upon visiting the banks' main website. A number of things can happen on mobile detection such as redirecting to an app store, redirection to a mobile banking specific website or providing a menu of mobile banking options for the user to choose from.

Object of Mobile Banking:-

The main part of every new invention is the object of that particular thing by with we can get that what is the entity behind that and in present situation without any profit giving material customer does not attract towards any business. Although each and every producers and users want money-making scheme, so the head of the all banks RBI has given some rules and regulation for adopting this new technology so that any banker does not get any type of chance to become dictator in his field.

RBI Guidelines on mobile banking transa ctions[4] 1. Regulatory and Supervisory Issues i. Only banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer mobile banking services. ii. The services shall be restricted only to customers of banks and holders of debit/credit cards issued as

per the extant Reserve Bank of India guide lines.

iii. Only Indian Rupee based domestic services shall be provided. Use of mobile banking ser vices for cross border transfers is strictly pro hibited.

iv. Banks may also use the services of Business Correspondent appointed in compliance with RBI guidelines, for extending this facility to their customers.

v. The guidelines issued by the Reserve Bank on 'Risks and Controls in Computers and Tele communications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will apply mutatis mutandis to mobile banking.

vi. The guidelines issued by Reserve Bank on "Know Your Customer (KYC)", "Anti Money Laundering (AML)" and combating the Financ ing of Terrorism (CFT) from time to time would be applicable to mobile based banking services also.

vii. Only banks who have implemented core bank ing solutions would be permitted to provide mobile banking services.

viii. Banks shall file Suspected Transaction Report (STR) to Financial Intelligence Unit - India (FID-IND) for mobile banking transactions as in the case of normal banking transactions.

2.Registration of customers for mobile service

i. Banks shall put in place a system of document based registration with mandatory physical pres ence of their customers, before commencing mobile banking service.

ii. On registration of the customer, the full details of the Terms and Conditions of the service of fered shall be communicated to the customer.

3. Technology and Security Standards

Information Security is most critical to the business of mobile banking services and its underlying operations. Therefore, technology used for mobile banking must be secure and should ensure confidentiality, integrity, authenticity and non-reputability.

4. Inter-operability

i. Banks offering mobile banking service must ensure that customers having mobile phones of any network operator is in a position to avail of the service. Restriction, if any, to the customers of particular mobile operator(s) is permissible only during the initial stages of offering the ser vice, up to a maximum period of six months subject to review.

ii. The long term goal of mobile banking frame work in India would be to enable funds transfer from account in one bank to any other account in the same or any other bank on a real time basis irrespective of the mobile network a cus tomer has subscribed to. This would require inter-operability between mobile banking ser vice providers and banks and development of a host of message formats. To ensure inter-oper ability between banks, and between their mo bile banking service providers banks shall adopt the message formats like ISO 8583, with suit able modification to address specific needs.

5. Clearing and Settlement for inter-bank funds transfer transactions

To meet the objective of a nation-wide mobile banking framework, facilitating inter-bank settlement, a robust clearing and settlement infrastructure operating on a 24x7 basis would be necessary. Pending creation of such a national infrastructure, banks may enter into bilateral or multilateral arrangement for inter-bank settlements, with express permission from Reserve Bank of India, wherever necessary.

6. Customer Complaints and Grievance Redressal Mechanism

The customer /consumer protection issues assume a special significance in view of the fact that the delivery of banking services through mobile phones is relatively new.

7. Transaction limit

i. A per transaction limit of Rs. 2500/- shall be imposed on all Mobile Banking transactions sub ject to an overall cap of Rs. 5000/- per day, per customer.

ii. Banks may also put in place monthly transac tion limit depending on the bank's own risk per ception of the customer.

8. Board approval

Approval of the Board of Directors (Local Board in case of foreign banks) for the product as also the related security policies must be obtained before launching the scheme.

9. Approval of Reserve Bank of India

Banks wishing to provide mobile banking services shall seek prior one time approval of the Reserve Bank of India, by furnishing full details of the proposal.

Security Measures to Be Taken By Banks and Mobile Networks to Prevent Mobile Banking Fraud: The security measures that must be adopted to prevent such threats have to be divided into two broad categories viz, the steps to be followed by the bank and those to be followed by the bank's customers. One important step that all banks can take is to provide an official mobile banking application to its customers that prevents them from using an application developed by another individual or entity. This helps users from falling into 'phishing' traps set by fraudulent developers.

Secondly, a secure and encrypted data transfer must be enabled between the user cell phone and the service provider, in this case, the telecom carrier. All further connections to the banks servers should be done through dedicated lines or virtual private networks. Thirdly, transactions that ask for credit or debit must pass through multiple levels of authentication such as authentication of the cell phone, the customer identification number and the secret mobile PIN or personal identification number allotted to a customer.

Fourthly, at any time during a transaction, the PIN must not be allowed to be transferred as plain text. It should be encrypted and must be interpreted only at the sending and receiving ends.?

Finding:

Role of Consumer protection Act

Consumer protection in India is covered by both statutory regulation and by voluntary membership bodies. Key players in consumer protection include the Reserve Bank of India (RBI), the Banking Codes and Standards Board of India (BCSBI), the Banking Ombudsman, the Indian Banking Association, and Consumer Courts as well as banks with internal customer service mechanisms.

First, RBI, a main regulator for banks and other financial institutions, establishes regulation and policy related to consumer protection. For instance, there are a number of circulars relating to fair practices at NBFCs. Additionally, the 2011 NBFC-MFI Directions include several provisions on pricing, transparency, recovery methods, and avoidance of multiple-borrowing. Secondly, banks play a role in consumer protection by adhering to RBI issued regulations and guidelines, such as the Grievance Redressal Mechanism in Banks of 2008. This circular advises banks to implement an internal customer service mechanism that receives and addresses complaints from its customers and resolves complaints in a fair and efficient manner. These guidelines, which are further explained in a model document released by the Indian Banks Association, are also stipulated by the BCSBI.

Similarly, the RBI Circular on the Use of Business Facilitators and Business Correspondents of 2006 requires each bank to establish "grievance redressal machinery" to redress complaints about services rendered by business correspondents and business facilitators and widely publicize this machinery through electronic and print media. These consumer-protection related requirements are further elaborated in the 2010 Guidelines for Engaging Business Correspondents.

In a majority of the states in India, the RBI has set up local Banking Ombudsmen, who act as arbiters of customers' disputes with banks. At an appellate level, ombudsmen handle complaints and grievances that have not been fully resolved by the banks or have not been adequately resolved in the opinion of the customer. The Consumer Protection Act No. 68 of 1986, which impacts financial institutions, established the Central Consumer Protection Council and the State and District Consumer Protection Councils, and establishes courts at the district, state, and national level for the resolution of customer disputes. Courts are located in district headquarters and do not require legal representation in order to press claims; however, customers may be reluctant to pursue these options due to the duration of decision-making and the likelihood that banks will simply appeal unfavorable outcomes.

The Banking Codes and Standards Board of India (BCSBI), which started as a collaborative venture between the banking industry and the RBI in 2005, serves as an independent and autonomous watchdog for the industry. The BCSBI is engaged in developing standards, improving transparency, and improving relations between banks and customers, and boasts over seventy member

banks. The BCSBI has developed the Banking Code Rules (covering member bank obligations to BCSBI) and the Code of Bank's Commitment to Customers Code (covering member bank commitments to customers), also referred to as the Fair Practices Code, with which all member banks must comply. The BCSBI also requires all banks to disseminate information to customers and manages a web-based helpline for customers although it is not widely used5.

Suggestions:

The instructions that banks should allocate6:

a. Always use a secured Wi-Fi connection, where you have a unique user name and password, before sending any sensitive information over your mobile phone.
b. Download your bank's mobile application from a legitimate app store associated with your phone and use it every time, so you can be sure you are visiting the real bank every time and not a copy cat site.
c. Install anti-malware technology, and back up data regularly.
d. Configure your device to auto-lock after a pe riod of time with a password of six-to-eight al phanumeric characters.
e. Keep your apps and device software up-to-date.

REFERENCE

1. KPMG "Monetizing Mobile" July 2011
2. "The World's first WAP Bank is Norwegian". itavisen.no. 1999-09-24. Retrieved 2010-10-18.
3. "A third of banks have mobile detection". Mapa Research. 2012-05-16. Retrieved
4. http://www.rbi.org.in
5. http://www.bu.edu
6. http://www.bankinfosecurity.com