Mobile Payment in India - Operative Guidelines for Banks

1. Introduction

1.1 With the rapid growth in the number of mobile phone subscribers in India (about 261 million as at the end of March 2008 and growing at about 8 million a month), banks have been exploring the feasibility of using mobile phones as an alternative channel of delivery of banking services. A few banks have started offering information based services like balance enquiry, stop payment instruction of cheques, record of last five transactions, location of nearest ATM/branch etc. Acceptance of transfer of funds instruction for credit to beneficiaries of same/or another bank in favor of pre-registered beneficiaries have also commenced in a few banks. Considering that the technology is relatively new and due care needs to be taken on security of financial transactions, there has been an urgent need for a set of operating guidelines that can be adopted by banks.

1.2 For the purpose of these Guidelines, “mobile payments” is defined as information exchange between a bank and its customers for financial transactions through the use of mobile phones. Mobile payment involves debit/credit to a customer’s account’s on the basis of funds transfer instruction received over the mobile phones.

1.3 Providing the framework for enabling mobile payments services to banking customers would generally involve the collaboration of banks, mobile payments service providers and mobile network operators (MNOs). The service can also be provided as a proximity payment system, where the transactions are independent of the MNOs. In mobile payment systems, the banks provide the basic service framework, ensure compliance to KYC/AML norms, creates a risk management and mitigation framework, and ensures settlement of funds. The mobile payments service providers are intermediaries for providing the technology framework for the implementation of the mobile payments services. The mobile network operators provide the telecom infrastructure and connectivity to the customers. Their role is limited to providing the SMS/WAP/GPRS/USSD/NFC GSM or CDMA voice and data services connectivity and in hosting the certain technology solutions like USSD. In a Non-MNO based systems, proximity or contactless channels like IRDA, RFID, Optical, NFC, etc. are used for communication between POS and the mobile phone of the customer.

1.4 As a first step towards building a mobile payment framework in India, these guidelines are meant only for banking customers – within the same bank and across the banks. It would be the responsibility of the banks offering mobile payment service to ensure compliance to these guidelines.

1.5 A brief description of the regulatory framework for mobile payments in a few countries is given at **Annex – I**.

2. Regulatory & Supervisory Issues

2.1 Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer mobile payment services to residents of India.

2.2 The services should be restricted to only to bank accounts/ credit card accounts in India which are KYC/AML compliant.

2.3 Only Indian Rupee based services should be provided.

2.4 Banks may use the services of Business Correspondents for extending this facility, to their customers. The guidelines with regard to use of business correspondent would be as per the RBI circular on Business correspondents issued from time to time.

2.5 The guidelines issued by RBI on 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will equally apply to Mobile payments, since Mobile devices used for this purpose have embedded computing and communication capabilities.

2.6 The RBI guidelines on "Know Your Customer (KYC)" and "Anti Money Laundering (AML)" as prescribed by RBI from time to time would be would be applicable to customers opting for mobile based banking service.

3. Registration of customers for mobile service

3.1 Banks should offer mobile based banking service only to their own customers.

3.2 Banks should have a system of registration before commencing mobile based payment service to a customer.

3.3 There can be two levels of mobile based banking service - the first or basic level in the nature of information like balance enquiry, SMS alert for credit or debit, status of last five transactions, and many other information providing services and the second or standard level in the nature of financial transactions such as payments, transfers and stop payments. The risk associated with the basic level of information services is much less compared to the standard level of actual payment services. Prior registration of the customers would be necessary irrespective of the type of service requested. For the standard level service one time registration should be done through a signed document.

4 Technology and Security Standards

4.1 The technology used for mobile payments must be secure and should ensure confidentiality, integrity, authenticity and non-repudiability. An illustrative, but not exhaustive framework is given at **Annex-II**.

4.2 The Information Security Policy of the banks may be suitably updated and enforced to take care of the security controls required specially for mobile phone based delivery channel.

5. Inter-operability

5.1 When a bank offers mobile payments service, it may be ensured that customers having mobile phones of any network operator should be in a position to request for service. Restriction, if any, to the customers of particular mobile operator(s) may be only during the pilot phase.

5.2 To ensure inter-operability between banks and between their mobile payments service providers, it is recommended that banks may adopt the message formats being developed by Mobile Payments Forum of India (MPFI). Message formats such as ISO 8583 , which is already being used by banks for switching of ATM transactions , may be suitably adapted for communication between switches where the source and destination are credit card/ debit cards/pre-paid cards.

5.3 The long term goal of mobile payment framework 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 mobile network a customer has subscribed to. This would require inter-operability between mobile payments service providers and banks and development of a host of message formats. Banks may keep this objective while developing solution or entering into arrangements with mobile payments solution providers.

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

6.1 For inter-bank funds transfer transactions, banks can either have bilateral or multilateral arrangements.

6.2 To meet the long term objective of a nation-wide mobile payment framework in India as indicated at para 5.3 above, a robust clearing and settlement infrastructure operating on a 24x7 basis would be necessary. Pending creation of such an infrastructure on a national basis, banks may enter in to multilateral arrangement and create Mobile Switches / Inter-bank Payment Gateways with expressed permission from RBI.

7. Customer Complaints and Grievance Redressal Mechanism

7.1 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. Some of the key issues in this regard and the legal aspects pertaining to them are given at **Annex-III**.

8. Need for Board level approval

8.1 Banks should get the Mobile payments scheme approved by their respective boards / Local board (for foreign banks) before offering it to their customers. The Board approval must document the extent of Operational and Fraud risk assumed by the bank and the bank's processes and policies designed to mitigate such risk.

8.2 banks who have already started offering mobile payment service may review the position and comply to these guidelines within a period of three months from issuance of these guidelines.

List of Abbreviations

AML	Anti Money Laundering
CDMA	Code Division Multiple Access
GPRS	General Packet Radio Service
GSM	Global System for Mobile
IDS	Intruder Detection System
IRDA	Infrared Data Association
ISO	International Standards Organization (Some times also written as International Organization for Standardization)
IVR	Integrated Voice Response
KYC	Know Your Customer
MNO	Mobile Network Operator
mPIN	Mobile Personal Identification Number
MPFI	Mobile Payment Forum of India
NFC	Near Field communication.
OTP	One Time Password
PCI-DSS	Payment Card Industry Data Security Standard
PIN	Personal Identification Number
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module
SMS	Short Messaging Service
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol

Annex-I

International Experience

There is very little material available on the regulatory frame work for mobile payments by central banks. Although there are a number of research articles available, they refer to the practices available rather than regulatory guidelines. Efforts to collect specific regulatory guidelines, from a few countries where person to person remittance through mobile channel has been implemented, have not been a success. Mobile payment framework in most countries is covered under the General Electronic Banking Guidelines. However, on the website of Consultative Group for Assisting the Poor(CGAP), there are several discussion papers on mobile payments. Examples of Kenya, Philippines, South Africa and Tanzania have been described in great detail. In these countries, cash-in and cash-out for the purpose of remittance is permitted to be done by the distributors of mobile companies. State Bank of Pakistan has also placed a 'Draft policy paper on Regulatory Framework for Mobile Payments in Pakistan' on their website for public comments.

Annex- II

Technology and Security Standards

The security controls/guidelines mentioned in this document are not exhaustive. The guidelines should be applied in a way that is appropriate to the risk associated with services provided by the bank through the mobile platform, the devices used, the delivery channels used (SMS, USSD, WAP, WEB, SIM tool kit based, Smart phone application based, IVR, IRDA, RFID, NFC, voice, etc) and the system which processes the mobile transactions and enables the interaction between the customers, merchants, banks and other participants.

2. The mobile payments could get offered through various mobile network operator based channels (SMS, USSD, WAP, WEB, SIM tool kit, Smart phone application based, IVR, voice, etc) and non MNO based proximity or contactless channels (IRDA, RFID, Optical, NFC, etc) and these various mobile channels offer various degrees of security and interaction capability. While the objective of the RBI is to have a fully functional digital certificate based inquiry/transaction capabilities to ensure the authenticity and non-repudiability, given the complexities involved in getting this through all the channels and given the need for enabling mobile payments to facilitate financial inclusion objectives, it is suggested that the banks evaluate each of these channels in terms of security and risks involved and offer appropriate services and transactions. Banks are also advised to provide appropriate risk mitigation measures like transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. per channel depending on the nature of the security features, risk perception by the bank offering the services and interaction capabilities.

3. It is suggested that the banks issue a new mobile pin (mPIN). To facilitate the mobile payments mPIN may be issued and authenticated by the bank or by a mobile payment application service provider appointed by the bank. Banks and the various service providers involved in the m-banking should comply with the following security principles and practices with respect to mPIN :

a) Implement a minimum of 4 digit customer mPIN (6 digit mPIN may be the desirable goal)

b) Protect the mPIN using end to end encryption

c) Do not allow the mPIN to be in clear text anywhere in the network or the system

d) Authenticate the mPIN in tamper-resistant hardware such as HSM

(hardware security modules)

e) Store the PIN in a secure environment

f) In case of offline authentication, the banks should ensure that a proper process is put in place to positively identify the customer the first time when the service is being enabled. An offline PIN may be used as the authentication parameter with security levels being as strong as in the case of online authentication. The bank may choose to issue its own offline PIN or adopt a customer-defined PIN.

g) A second factor of authentication may be built-in for additional security and as such the second factor can be of the choosing of the bank

4. All transactions that affect an account (those that result in to an account being debited or credited, including scheduling of such activity, stop payments, etc) should be allowed only after authentication of the mobile number and the mPIN associated with it in case of MNO based payment service. In case of Non-MNO based mobile proximity payment, specific static or dynamic identifier should be used as second factor authentication along with mPIN.. Two factor authentication may be adopted even for transactions of information nature such as balance enquiry, mini statements, registered payee details. ,

5. Proper system of verification of the mobile phone number should be implemented, wherever possible. This is to guard against spoofing of the phone numbers as mobile phones would be used as the second factor authentication. It may also be suggested but not mandatory, that either card number or OTP (one time passwords) be used as the second factor authentication rather than the phone number.

6. Proper level of encryption should be implemented for communicating from the mobile handset to the bank's server or the server of the mobile payments service provider, if any. Proper security levels should be maintained for transmission of information between the bank and the mobile payments service provider. The following guidelines with respect to network and system security should be adhered to:

a) Use strong encryption for protecting the sensitive and confidential information of bank and customers in transit

b) Implement application level encryption over network and transport layer encryption wherever possible.

c) Establish proper firewalls, intruder detection systems (IDS), data file and system integrity checking, surveillance and incident

response procedures and containment procedures.

d) Conduct periodic risk management analysis, security vulnerability assessment of the application and network etc at least once in a year.

e) Maintain proper and full documentation of security practices, guidelines, methods and procedures used in mobile payments and payment systems and keep them up to date based on the periodic risk management, analysis and vulnerability assessment carried out.

f) Implement appropriate physical security measures to protect the system gateways, network equipments, servers, host computers, and other hardware/software used from unauthorized access and tampering. The Data Centre of the Bank and Service Providers should have proper wired and wireless data network protection mechanisms.

7. The dependence of banks on mobile payments service providers may place knowledge of bank systems and customers in a public domain. Mobile payment system may also make the banks dependent on small firms (i.e mobile payment service providers) with high employee turnover. It is therefore imperative that sensitive customer data, and security and integrity of transactions are protected. It is necessary that the mobile payments servers at the bank's end or at the mobile payments service provider's end, if any, should be certified appropriately, say through a PCI DSS certification or in compliance with each participant banks security guidelines. In addition, banks should conduct regular information security audits on the mobile payments systems to ensure complete security. Further, if a mobile payments service provider aggregates and processes transaction, including verification of mPINs, additional security measures such as a Hardware Security Module (HSM) must be deployed over and above link encryption to ensure that mPIN data is protected adequately.

8. It is recommended that for channels such as WAP and WEB which do not contain the phone number as identity, a separate login ID and password be provided as distinct from the internet banking either by bank or the payment service provider. It is recommended that Internet Banking login ids and passwords may not be allowed to be used through the mobile phones. Allowing Internet banking login id and password usage on the mobile phone may compromise their usage on the Internet banking channel. This restriction may be communicated to the customers while offering mobile payments service. However, Internet Banking login ids and passwords can allowed to be used through the mobile phones provided a) https connectivity through GPRS is used and b) end to end encryption of the password and customer sensitive information happens.

9. Plain text SMS is the simplest form of communication through mobile phones, but is vulnerable to tampering. As long as there is a second level of check on the details of the transaction so as to guard against data tampering this mode of communication can be used for financial messages of micro payment transactions (say about rupees One thousand five hundred) and repetitive utility bill payment transactions (say not exceeding rupees two thousand five hundred).

Annex-III

Customer Protection Issues

Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening a savings / current account can be accepted over Mobile Telecommunication, these should be opened only after proper introduction and physical verification of the identity of the customer using prevalent KYC norms.

2. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, provides for a particular technology as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk. Customers must be made aware of the said legal risk prior to sign up.

3. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers‘ accounts. In the mobile payments scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may 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 risks.

4. As in an Internet banking scenario, in the mobile payments scenario too, there is very limited or no stop-payment privileges for mobile payments transactions since it becomes impossible for the banks to stop payment in spite of receipt of stop payment instruction as the transactions are completely instantaneous and are incapable of being reversed. Hence, banks offering mobile payments should clearly notify the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.

5. 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 mobile payments services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks’ liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Mobile payments should consider insuring themselves against such risks, as is the case with Internet Banking.

6. Bilateral contracts between the payee and payee's bank, the participating banks and service provider and the banks themselves will form the legal basis for mobile transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law. It is likely that there will be two sets of contracts; one would be a commercial contract between service providers and the second, a contract between the customer and the bank, to provide a particular service/ s. At all time, legal obligations of each party must be made clear through these contracts.

7. Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Mobile phone, through a disclosure template on their websites and/or through printed material.

8. The existing mechanism for handling customer complaints / grievances may be used for mobile payment transactions as well. However, the technology is relatively new, banks offering mobile payment service should set up a help desk and make the details of the help desk and escalation procedure for lodging the complaints, if any public on their websites. Such details should also be made available to the customer at the time of sign up.

9. In cases where the customer files a complaint with the bank disputing a transaction, it would be the responsibility of the service providing bank, to address the customer grievance. Banks may formulate chargeback procedures for addressing such customer grievances.

10. Banks may also consider covering the risks arising out of fraudulent/disputed transactions through appropriate insurance schemes.

11. The jurisdiction of legal settlement would be within India.