Mobile Banking transactions in India - Operative Guidelines for Banks

1. Introduction

1.1 Mobile phones as a medium for extending banking services have off-late been attaining greater significance. The rapid growth in users and wider coverage of mobile phone networks have made this medium an important platform for extending banking services to customers. 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. Some banks have started offering information based services like balance enquiry, stop payment instruction of cheques, transactions enquiry, location of the 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. In order to ensure a level playing field and considering that the technology is relatively new, Reserve Bank has brought out a set of operating guidelines for adoption by banks.

1.2 For the purpose of these Guidelines, "mobile banking transactions" is undertaking banking transactions using mobile phones by bank customers that involve credit/debit to their accounts.

2. Regulatory & Supervisory Issues

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

2.2 The services shall be restricted only to customers of banks and/or holders of debit/credit cards issued as per the extant Reserve Bank of India guidelines.

2.3 Only Indian Rupee based domestic services shall be provided. Use of mobile banking services for cross border inward and outward transfers is strictly prohibited.

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

2.5 The guidelines issued by the Reserve Bank 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 apply mutatis mutandis to mobile banking.

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

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

2.8 Banks shall file Suspicious Transaction Report (STR) to Financial Intelligence Unit – India (FIU-IND) for mobile banking transactions as in the case of normal banking transactions.

3. Registration of customers for mobile service

3.1 Banks shall put in place a system of document based registration with mandatory physical presence of their customers, before commencing mobile banking service. Reserve Bank would consider relaxation in specific cases while approving the proposals of banks.

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

4 Technology and Security Standards

4.1 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-repudiability. An illustrative, but not exhaustive framework is given at **Annex-I**.

5. Inter-operability

5.1 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 service, up to a maximum period of six months subject to review.

5.2 The long term goal of mobile banking 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 the mobile network a customer has subscribed to. This would require inter-operability between mobile banking service providers and banks and development of a host of message formats. To ensure inter-operability between banks, and between their mobile banking service providers, banks shall adopt the message formats like ISO 8583, with suitable modification to address specific needs.

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

6.1 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, unless such arrangements have been authorized by the Reserve Bank under the Payment and Settlement System Act, 2007.

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 are given at **Annex-II**.

8. Transaction limit

8.1 For the present, banks are permitted to offer this facility to their customers subject to a daily cap of Rs. 5000/- per customer for funds transfer and Rs.10,000/- per customer for transactions involving purchase of goods/services.

8.2 Banks may also put in place monthly transaction limit depending on the bank's own risk perception of the customer.

9. Board approval

9.1 Approval of the Board of Directors (Local Board in case of foreign banks) for the product, as also the perceived risks and mitigation measures proposed to be adopted must be obtained before launching the scheme.

10. Approval of Reserve Bank of India

10.1 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.

Annex- I

Technology and Security Standards

1. The security controls/guidelines mentioned in this document are only indicative. However, it must be recognised, the technology deployed is fundamental to safety and soundness of any payment system. Therefore, banks are required to follow the Security Standards appropriate to the complexity of services offered, subject to following the minimum standards set out in this document. The guidelines should be applied in a way that is appropriate to the risk associated with services provided by the bank and the system which supports these services.

2. Banks are required to put in place appropriate risk mitigation measures like transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. depending on the bank's own risk perception, unless otherwise mandated by the Reserve Bank.

3**. Authentication**
Banks providing mobile banking services shall comply with the following security principles and practices for the authentication of mobile banking transactions:

a) All mobile banking shall be permitted only by validation through a two factor authentication.

b) One of the factors of authentication shall be mPIN or any higher standard.

c) Where mPIN is used, end to end encryption of the mPIN is desirable, i.e mPIN shall not be in clear text anywhere in the network.

d) The mPIN shall be stored in a secure environment.

4. Proper level of encryption and security shall be implemented at all stages of the transaction processing. The endeavor shall be to ensure end-to-end encryption of the mobile banking transaction. Adequate safe guards would also be put in place to guard against the use of mobile banking in money laundering, frauds etc. The following guidelines with respect to network and system security shall be adhered to:

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

b) Establish proper firewalls, intruder detection systems (IDS), data file and system integrity checking, surveillance and incident response procedures and containment procedures.

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

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

e) 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.

5. The dependence of banks on mobile banking service providers may place knowledge of bank systems and customers in a public domain. Mobile banking system may also make the banks dependent on small firms (i.e mobile banking 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 banking servers at the bank's end or at the mobile banking service provider's end, if any, should be certified by an accredited external agency. In addition, banks should conduct regular information security audits on the mobile banking systems to ensure complete security.

6. For mobile banking facilities which do not contain the phone number as identity, a separate login ID and password is desirable to ensure proper authentication.

Annex-II

Customer Protection Issues

1. Any 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 is a source of legal risk. Customers must be made aware of the said legal risk prior to sign up.

2. Banks are required to maintain secrecy and confidentiality of customers' accounts. In the mobile banking scenario, the risk of banks not meeting the above obligation is high. Banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., on account of hacking/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks.

3. As in an Internet banking scenario, in the mobile banking scenario too, there is very limited or no stop-payment privileges for mobile banking 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 banking should notify the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.

4. 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 banking services are being determined by bilateral agreements between the banks and customers. Taking into account the risks arising out of unauthorized transfer through hacking, denial of service on account of technological failure etc. banks providing mobile banking would need to assess the liabilities arising out of such events and take appropriate counter measures like insuring themselves against such risks, as in the case with internet banking.

5. Bilateral contracts drawn up between the payee and payee’s bank, the participating banks and service provider should clearly define the rights and obligations of each party.

6. Banks are required to make mandatory disclosures of risks, responsibilities and liabilities of the customers on their websites and/or through printed material.

7. The existing mechanism for handling customer complaints / grievances may be used for mobile banking transactions as well. However, in view of the fact that the technology is relatively new, banks should set up a help desk and disclose the details of the help desk and escalation procedure for lodging the complaints, on their websites. Such details should also be made available to the customer at the time of sign up.

8. 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 expeditiously redress the complaint. Banks may put in place procedures for addressing such customer grievances. The grievance handling procedure including the compensation policy should be disclosed.

9. Customers complaints / grievances arising out of mobile banking facility would be covered under the Banking Ombudsman Scheme.

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