भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2016-17/17
DPSS.CO.PD.Mobile Banking.No./2/02.23.001/2016-2017 July 1, 2016
(Updated as on November 12, 2021)
(Updated as on January 10, 2020)

The Chairman and Managing Director / Chief Executive Officers
All Scheduled Commercial Banks including RRBs /
Urban Co-operative Banks / State Co-operative Banks /
District Central Co-operative Banks

Madam /Dear Sir,

Master Circular – Mobile Banking transactions in India – Operative Guidelines for Banks

As you are aware, the Reserve Bank of India has, from time to time, issued a number of circulars containing guidelines on Mobile Banking. This Master Circular has been prepared to facilitate the banks and other stakeholders to have all the extant instructions on the subject at one place.

2. The Master Circular has been updated by incorporating all the instructions/guidelines issued on Mobile Banking up to December 17, 2015 and has been placed on the RBI web-site (http://www.rbi.org.in). A list of circulars finding reference in this master circular is enclosed as Appendix.

Yours faithfully,

(Nanda Dave)
Chief General Manager

Contents

Master Circular – Mobile Banking

1. Purpose

To provide a consolidated document containing all rules / regulations / procedures prescribed to be followed by banks for operationalising Mobile Banking in India.

2. Classification

Statutory Guidelines issued by Reserve Bank of India under section 18 of Payment & Settlement Systems Act, 2007, (ACT 51 of 2007).

3. Previous Guidelines consolidated

The Master Circular compiles the instructions contained in the circulars issued on Mobile Banking as listed in **Appendix.**

4. Scope

The guidelines are applicable to all commercial banks (including Regional Rural Banks), Urban Cooperative Banks, State Cooperative Banks and District Central Cooperative Banks.

5. Introduction

5.1 Mobile phones, as a medium for extending banking services, have attained greater significance because of their ubiquitous nature. The rapid growth of mobile users in India, through wider coverage of mobile phone networks, have made this medium an important platform for extending banking services to every segment of banking clientele in general and the unbanked segment in particular.

5.2 In order to ensure a level playing field, Reserve Bank brought out a set of operating guidelines for adoption by banks. The guidelines, finalised following a wide consultative process with the stakeholders, were first issued in October 2008 and since then have been updated keeping in view the developments taking place.

5.3 For the purpose of the instructions contained in this Master Circular, 'Mobile Banking transaction' means undertaking banking transactions using mobile phones by bank customers that involve accessing / credit / debit to their accounts

5.4 Banks are permitted to offer mobile banking services (through SMS, USSD or mobile banking application) after obtaining necessary permission from the

Department of Payment & Settlement Systems, Reserve Bank of India. Mobile Banking services are to be made available to bank customers irrespective of the mobile network.

6. Regulatory & Supervisory Issues

6.1 Banks which are licensed, supervised and having physical presence in India, are permitted to offer mobile banking services. Only banks who have implemented core banking solutions are permitted to provide mobile banking services.

6.2 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.

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

6.4 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.

6.5 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.

6.6 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.

7. Registration of customers for mobile service

7.1 Banks shall put in place a system of registration of customers for mobile banking. Banks should strive to provide options for easy registration for mobile banking services to their customers, through multiple channels, thus minimizing the need for the customer to visit the branch for such services. The time taken between registration of customers for mobile banking services and activation of the service should also be minimal.

7.2 The system put in place by banks for registration of customers for mobile banking for new as well as existing account holders (where mobile number is either registered with the bank or is not available) , is varied across banks. Thus, there is a need for greater degree of standardization in procedures relating to the above particularly when customers are using inter-operable mobile banking platforms. Few best practices that can be adopted by banks for registering / on-boarding customers for mobile banking, under the scenarios indicated above, are given in the Annex-I

7.3 - With a view to simplify the procedure of registration for Mobile Banking, Reserve Bank of India has advised National Payment Corporation of India (NPCI) to develop the mobile

banking registration service / option on National Financial Switch (NFS). Accordingly all banks shall carry out necessary changes in their respective ATM switches to enable customer registration for mobile banking at all their ATMs. (Circular DPSS.CO.PD. No./1265/02.23.001/2015-2016 dated December 17, 2015)

7.4 In order to address the challenges in extending the facility of MPIN generation to the customers registered for mobile banking, banks have to explore various options. In order to quicken the process of MPIN generation and also widen the accessibility to their mobile banking registered customers, banks can consider adopting various channels / methods such as

a. Through the ATM channels (similar to option available for change of PIN on their own ATMs as well as in inter-operable ATM networks)
b. Through an option provided in the USSD menu for mobile banking (both their own USSD platform, if any, as well as under the inter-operable USSD Platform for mobile banking)
c. Banks' own internet banking website, with necessary safeguards
d. Use of MPIN mailers (like PIN mailers for cards)
e. Common website can also be designed as an industry initiative

7.5. Banks may also undertake customer education and awareness programme in multiple languages through different channels of communication to popularise their process of mobile banking registration/activation and its usage etc.

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

8. Technology and Security Standards

8.1 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.

8.2 Transactions up to Rs 5000/- can be facilitated by banks without end-to-end encryption. The risk aspects involved in such transactions may be addressed by the banks through adequate security measures. (Circular DPSS.CO.No.2502/02.23.02/ 2010-11 dated May 4, 2011)

8.3 An illustrative framework for technology and security is given at **Annex- II**.

9. Inter-operability

9.1 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, i.e. should be network independent. Restriction, if any, for the customers of particular mobile operator(s) are permissible only during the initial stages of offering the service, up to a maximum period of six months subject to review.

9.2 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 interoperability 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.

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

10.1 To meet the objective of nation-wide mobile banking framework facilitating inter-bank settlement, a robust clearing and settlement infrastructure operating on a 24x7 basis is necessary. Bank and non-bank entities putting such systems in place, bilateral or multilateral, need authorisation from Reserve Bank of India, under the Payment and Settlement System Act, 2007.

11. Customer Complaints and Grievance Redressal Mechanism

11.1 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-III**.

12. Transaction limit

12.1 Banks are permitted to offer mobile banking facility to their customers without any daily cap for transactions involving purchase of goods/services. (Circular DPSS.CO.PD.No.1098/02.23.001/2011-12 dated December 22, 2011).

12.2 However, banks may put in place per transaction limit depending on the bank's own risk perception, with the approval of its Board.

13. Remittance of funds for disbursement in cash

13.1 In order to facilitate the use of mobile phones for remittance of cash, banks are permitted to provide fund transfer services which facilitate transfer of funds from the accounts of their customers for delivery in cash to the recipients. The disbursal of funds to recipients of such services can be facilitated at ATMs or through any agent(s) appointed by the bank as business correspondents. The recipient can be a

non -account holder also. (Circular DPSS.CO.No.1357/02.23.02/2009-10 dated December 24, 2009)

13.2 Such fund transfer service shall be provided by banks subject to the following conditions:-

a) In case of cash out, the maximum value of such transfers shall be Rs 10,000/- per transaction. Banks may place suitable cap on the velocity of such transactions, subject to a maximum value of Rs 25,000/- per month, per beneficiary (Circular DPSS.CO.PD.No.622/02.27.019/2011-12 dated October 5, 2011).
b) The disbursal of funds at the agent/ATM shall be permitted only after identification of the recipient. In this connection, attention of banks is drawn to the provisions of the Notification dated November 12, 2009, issued by Government of India, under Prevention of Money Laundering Act, 2002, as amended from time to time.
c) Banks may carry out proper due diligence of the persons before appointing them as authorized agents for such services.
d) Banks shall be responsible as principals for all the acts of omission or commission of their agents.

14. Board approval

14.1 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.

15. Approval of Reserve Bank of India

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

Annex-I

Suggestions / best practices for increasing the penetration (customer registration / on-boarding) of Mobile Banking

1. New Customer: at account opening time

a. Account opening form should clearly indicate the option for mobile banking – the option for mobile banking services should be clear and distinct from the contact details of the customer where mobile number is also accepted; it should also be clearly indicated that alerts (if sent through SMS) will be sent to this registered mobile number.
b. Customer should be made aware of the mobile banking facilities while opening the account. Further, the form should also clearly indicate that opting for mobile banking services will provide an alternate delivery channel to the customer; related inputs / materials / booklet etc. should be provided to the interested customers outlining the features of mobile banking services offered by the bank, the process involved, roles and responsibilities etc.

2. Existing Customer- Mobile numbers registered with the bank but not active for mobile banking:

As mobile number registration has already taken place and available with the bank (is linked with the account), wider and more accessible platforms should also be made use of by the banks to increase awareness on mobile banking at every opportunity to get more and more customers to register for mobile banking services. Some of the methods that can be adopted by banks for having targeted customer awareness programs could include:

i. sending SMS / e-mails to their customers on registered mobile numbers / e-mail ids about activating mobile banking, providing necessary URLs / customer care numbers from which the customer can obtain additional information on mobile banking activation process;
ii. ATMs and self-service Kiosks at branches can also alert the customers to activate the mobile banking options;
iii. social media can also be used by the banks to build awareness and encourage customers to register on mobile banking;
iv. through the internet banking website of the bank especially when the customer logs in for net banking operations (taking into account the security architecture and authentication mechanism already prevalent in the bank/s);

v. banks can use their IVR and phone banking channels to encourage and facilitate registration and activation of customers for mobile banking;

vi. banks can also harness the potential of inter-operable channels such as the NFS (which is widely used by customers for transacting with their cards) to provide a widely accessible channel for mobile banking registration.

3. Existing Customer- Mobile number not registered with the bank at all

Banks need to find ways of obtaining mobile numbers of the account holders first for registration in their database and subsequently for mobile banking registration. Some of the options that can be used for this purpose are:

a. Through ATM channel – an alert / message can be given (at the ATM itself) by banks when the customer transacts at the ATM, that she/he has not registered any mobile number with the bank

b. Branch visit- at teller level, when the customer comes to the teller for any cash deposit / withdrawal transaction, the customer profile should indicate that he/she has not registered the mobile number at the bank and should be asked to do so immediately

c. Similarly, at passbook printing counters / kiosks too, the customer profile should be verified for existence of mobile number and customer should be advised to register the mobile number when he/she uses the passbook printing kiosk

d. At BC level with biometric authentication.

Annex- II

Technology and Security Standards – An Illustrative Framework

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 transactions involving debit to the account 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.
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-III

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 Reserve Bank - Integrated Ombudsman Scheme, 2021 (as amended from time to time).

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

Appendix

List of Circulars consolidated for the Master Circular

Sr. No.	Circular No.	Date	Subject
1.	DPSS.CO.No.619/02.23.02/2008-09	08.10.2008	Mobile Banking Transactions in India - Operative Guidelines for Banks
2.	DPSS.CO.No.1357/02.23.02/2009-10	24.12.2009	Mobile Banking Transactions in India - Operative Guidelines for Banks
3.	DPSS.CO.No.2502/02.23.02/2010-11	04.05.2011	Mobile Banking Transactions in India - Operative Guidelines for Banks
4.	DPSS.PD.CO.No.622/02.27.019/2011-2012	05.10.2011	Domestic Money Transfer-Relaxations
5.	DPSS.CO.PD.No.1098/02.23.02/2011-12	22.12.2011	Mobile Banking Transactions in India - Operative Guidelines for Banks
6.	DPSS.CO.PD.No.1017/02.23.02/2014-15	04.12.2014	Mobile Banking Transactions in India - Operative Guidelines for Banks
7.	DPSS.CO.PD.No./1265/02.23.001/2015-2016	17.12.2015	Mobile Banking Transactions in India - Operative Guidelines for Banks- Customer Registration for Mobile Banking