THE JANATA CO-OPERATIVE BANK LTD.

H.O.32, Netaji Subhash Marg, Darya Ganj, New Delhi-110 002
Telephones : 23256272-74, **E-mail** : ho-manager@janatabank.in

Mobile Banking Policy

The Mobile Banking Policy has been framed by the Audit Performance Review and Computer Mechanization Sub-Committee Committee taking into consideration the guidelines/circulars issued by Reserve Bank of India vide Circular No. 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) and approved by the BoM/Board of Directors in its meeting held on 20.03.2024/30.03.2024 vide Resolution No.A.1(a)(xiv) as under:

1. Introduction

To provide a consolidated document containing all rules / regulations / procedures prescribed to be followed by banks for operationalising Mobile Banking /internet banking facility to their customers should comply with the following;

(i) The bank should formulate a policy for Internet Banking with the approval of the Board.

(ii) The policy should fit into the bank's overall Information technology and Information Security Policy and ensures confidentiality of records and security systems.

(iii) The policy should clearly lay down the procedure to be followed in respect of 'Know Your Customer' requirements.

(iv) The policy should cover technology and security standards and also address the legal, regulatory and supervisory issues as enumerated in this Annex.

(v) The banks should put in place sound internal control systems and take into account the operational risks involved in providing the service.

(vi) Adequate disclosure should be made regarding the risk, responsibilities and liabilities to the customers before offering the facility

(vii) Mobile phones, as a medium for extending banking services, have of-late 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.

(viii) 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.

(ix) Bank have been permitted to offer mobile banking services after obtaining necessary permission from the Department of Payment & Settlement Systems, Reserve Bank of India. Mobile Banking services are available to bank customers irrespective of the mobile network. Customers need to first register for Mobile Banking with the bank and download the Mobile Banking application on his / her mobile handsets.

2. Regulatory & Supervisory Issues

(i) Bank have implemented core banking solutions and is permitted to provide mobile banking services.

(ii) The services shall be restricted only to customers of bank and/or holders of debit cards issued by the bank.

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

(iv) 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.

(v) 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.

(vi) Bank 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

(i) Bank shall put in place a system of document-based registration with mandatory physical presence 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 offered by the bank shall be communicated to the customer.

4. Technology and Security Standards

i) 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.

ii) 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 No.DPSS.CO.No.2502/02.23.02/ 2010-11 dated May 4, 2011)

5. Inter-operability

i) Bank offering mobile banking service must ensure that customers having mobile phones of any network operator are in a position to avail 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.

ii) 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.

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

To meet the objective of nation-wide mobile banking framework facilitating interbank settlement, a robust clearing and settlement infrastructure operating on a 24x7 basis is necessary. Bank has been authorised to put such systems in place from NPCI, under the Payment and Settlement System Act, 2007

8. 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. Some of the key issues in this regard are given at Annex-I.

9. Transaction limit

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

ii) However, bank have put in place per transaction limit depending on the bank's own risk perception, with the approval of its Board.

9. Technology and Security Standards

Bank has 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.

10. Authentication

i) Bank is 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 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.

ii) 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 equipment, 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.

iii) 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.

10. Conclusion

This policy will be taken up for review as and when there are major changes in the environment arising out of changes in the policy by Reserve Bank of India on Mobile Banking. However, in the absence of any such changes in the economic and banking scenario, this policy will continue to be in force. The changes made by the RBI and Government of India must be complied with and the Policy shall be revised, rectified and amended accordingly. This policy has been framed and shall be valid till it is revised.

For The Janata Co-operative Bank Ltd.

(P.S. Pathania)
Managing Director

THE JANATA CO-OP. BANK LTD. 32, F.F. N.S. MARG DARYAGANJ NEW DELHI

Annex-I

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 signup.

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.