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

RBI/2015-16/242
DBR.RRB.BC.No. 59/31.01.001/2015-16 **November 19, 2015**

All Regional Rural Banks

Dear Sir/Madam,

Internet Banking Facility for Customers of Regional Rural Banks

Presently, Regional Rural Banks (RRBs) are not permitted to provide internet banking facilities to their customers. With a view to enhancing customer service and taking into account demand for such services, it has been decided to allow RRBs to extend the facility of internet banking to their customers. The guidelines applicable to all the Regional Rural Banks are as follows:

I. Internet Banking (View only) facility

2. All RRBs which have implemented Core Banking Solution (CBS) and migrated to Internet Protocol Version 6 (IPv6) and complying with the guidelines prescribed in Annex-I to this circular may offer Internet Banking (View only) facility to their customers, without prior approval of RBI. In case, any service offered under 'view only' facility requires two-factor authentication or One Time Password (OTP), banks may adopt the security features prescribed in Annex II to this circular, as appropriate to such services.

3. The RRBs offering Internet Banking (View only) facility to their customers should ensure that the facility is strictly for non-transactional services such as balance enquiry, balance viewing, account statement download, request for supply of cheque books, etc. and no online fund-based transactions are allowed.

4. The RRBs have to report commencement of the service to the concerned Regional Office of RBI and NABARD within one month of operationalization of Internet Banking (View only) facility.

बैंकिंग विनियमन विभाग, केंद्रीय कार्यालय, 12वीं और 13वीं मंज़िल, केंद्रीय कार्यालय भवन, शहीद भगत सिंह मार्ग, मुंबई 400001
टेलीफोन /Tel No: 22661602, 22601000 फैक्स/Fax No: 022-2270 5670, 2260 5671, 5691 2270, 2260 5692
Department of Banking Regulation, Central Office, 12th & 13th Floor, Central Office Bhavan, Shahid Bhagat Singh Marg, Mumbai - 400001. Tel No: 22661602, 22601000 Fax No: 022-2270 5670, 2260 5671, 5691 2270, 2260 5692
हिंदी आसान है, इसका प्रयोग बढ़ाइए

II. Internet Banking with Transactional facility

5. All RRBs which have implemented CBS and have also migrated to Internet Protocol Version 6 (IPv6) and fulfilling the following criteria may offer Internet Banking with transactional facility to their customers with prior approval of RBI:

a. CRAR of not less than 10 per cent.
b. Networth is Rs.100 crore or more as on March 31 of the immediate preceding financial year.
c. Gross NPAs less than 7 % and Net NPAs not more than 3%
d. The bank should have made a net profit in the immediate preceding financial year and overall, should have made net profit at least in three out of the preceding four financial years.
e. It should not have defaulted in maintenance of CRR/SLR during the immediate preceding financial year.
f. The bank has a track record of regulatory compliance and no monetary penalty has been imposed on the bank for violation of RBI directives/guidelines during the two financial years, preceding the year in which the application is made.
g. It has sound internal control system which should be approved by a CISA qualified independent auditor.
h. The bank should not have accumulated losses.

6. RRBs fulfilling the above-mentioned criteria will be allowed to extend Internet Banking with transactional facility provided they comply with the guidelines prescribed in Annex I and II to this circular. For this purpose, the intending RRB shall submit an application to the concerned Regional Office of RBI through NABARD with the following documents:

i. A copy of the Board approved policy on internet banking along with a certificate from an independent auditor (CISA qualified) that the IT and IS policy requirements prescribed in RBI guidelines have been adhered to.
ii. An undertaking to inform RBI about any material change in the services/products offered by them.
iii. The business plan, cost and benefit analysis, operational arrangements like technology adopted, business partners, third party service providers and systems and control procedures that the bank proposes to adopt for managing risks.

7. The bank will report to the concerned Regional Office of RBI and NABARD every breach or failure of security systems and procedures and the latter, at its discretion, may decide to commission a special audit/inspection of such bank.

Yours faithfully,

(Sudha Damodar)
Chief General Manager

Encl: As above

Annex-I

Guidelines on Internet Banking facility to Customers of Regional Rural banks (RRBs)

RRBs intending to offer 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 bank 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.

Accordingly, the following guidelines are issued for implementation by the bank.

I. Technology and Security Standards:

a. RRBs should have appropriate Information Security policy duly approved by the Board of Directors. There should be clear segregation of duties between the Information Technology (IT) Division and the Information Security (IS) Division. The Information Technology Division will actually implement the computer systems. There should be a separate Information Security Officer dealing exclusively with Information Systems security. Further, an Information Systems Auditor will audit the Information Systems.
b. The bank should designate a Network and Database Administrator with clearly defined roles as per the IS Audit policy duly approved by their Board.
c. Logical access controls to data, Systems, Application software, utilities, telecommunication lines, libraries, System software, etc. should be in place.
d. The bank should ensure that there is no direct connection between the Internet and the bank's system.
e. The bank should have effective safeguards to prevent intrusions into the systems/network.
f. All unnecessary services on the Application Server such as File Transfer Protocol (FTP), Telnet should be disabled. The Application Server should be isolated from the e-mail server.

g. All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be recorded and follow up action taken. Banks should acquire tools for monitoring Systems and networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The bank should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies.

h. The Information Security officer and the Information System auditor should conduct periodic penetration tests of the system, which should include:

   1. Attempting to guess passwords using password-cracking tools.
   2. Search for back door traps in the programs.
   3. Attempt to overload the System using Distributed Denial of Service (DDoS) & Denial of Service (DoS) attacks.
   4. Check if commonly known holes in the software, especially the browser and the e-mail software exist.
   5. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers').

i. Physical access controls should be strictly enforced. Physical security should cover all the Information Systems and sites where they are housed, both against internal and external threats.

j. The bank should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as spelt out in the bank's security policy. Business continuity should be ensured by setting up Disaster Recovery sites. These facilities should also be tested periodically.

k. All applications should have proper record keeping facilities for legal purposes. It shall be necessary to keep all Received and Sent messages both in encrypted and decrypted form.

l. The bank shall obtain application integrity statement from the vendor/service provider, before implementing the internet banking software.

m. Security infrastructure should be properly tested before using the Systems and Applications for normal operations. Banks should periodically upgrade the Systems to newer versions which give better security and control.

n. 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 and DBS.CO.ITC.BC.No.6/31.02.008/2010-11 dated April 29, 2011 regarding Recommendations of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (Chairman: Shri G. Gopalakrishna, Executive Director);

advising banks to comply with the same, will equally apply to Internet banking, and guidelines on 'Introduction of IS Audit Policy' in NABARD circular NB.DoS.HO.POL.No. 3634/J-1/2014-15 dated February 25, 2015 will also apply.

II. Legal Issues

a. Banks may provide Internet Banking facility to a customer only at his/her option based on specific written or authenticated electronic requisition along with a positive acknowledgement.
b. Considering the prevailing legal position, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about the integrity and reputation of the customer opting for internet banking. Therefore, even though request for opening an account may be accepted over Internet, accounts should be opened only after verification of the identity of the customer and adherence to KYC guidelines.
c. From a legal perspective, security procedure adopted by banks for authenticating a user needs to be recognized by law as a substitute for signature. The provisions of the Information Technology Act, 2000, and other legal requirements need to be scrupulously adhered to while offering internet banking.
d. Under the present regime, there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts/information. In the Internet banking 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 / technological failures. The bank should, therefore, have in place adequate risk control measures to manage such risks.

III. Internal Control System

The bank should develop sound internal control systems before offering internet banking. This would include internal inspection / audit of systems and procedures related to internet banking as also ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data. Banks may also consider prescribing suitable monetary limits for customers on transactions put through internet banking. The internal control system should cover the following:

a. Role and Responsibilities / Organisational structure: The Board of Directors and senior management are responsible for ensuring that the internal control system operates effectively. Audit Committee of the Board should have a designated member with requisite knowledge of Information Systems, related controls and audit issues.

b. Audit Policy to include IS Audit: IS audit should be an integral part of the internal audit of banks. The bank should put in place a system to ensure that a robust audit trail is generated to facilitate conduct of audit, serving as forensic evidence when required and assist in dispute resolution.

c. Reporting and Follow-up: This involves having a system of reporting by the functionaries to the higher authorities. Any breach or failure of security systems and procedures will be reported to the next higher authority and to the Audit Committee. IS Auditors will prepare an audit summary memorandum providing overview of the entire audit processing from planning to audit findings, discuss the findings with auditee and obtain responses. The RRBs should have a time bound follow-up policy for compliance with audit findings. The Board of Directors need to be kept informed of serious lapses in security and procedures.

Banks may have a communication plan for escalating/reporting to the Board/Senior Management/ RBI/NABARD to proactively notify major cyber security incidents.

IV. Other Issues and Disclosures:

The existing regulatory framework for banks will be extended to Internet Banking also. In this regard, it is advised that:

a. The products under internet banking should be restricted to account holders only.
b. The services should include only local currency products.
c. RRBs should make disclosure of risks, responsibilities and liabilities of customers in doing banking through internet.
d. The banks need to adhere to the KYC guidelines / AML standards and the provisions and directions issued under the PMLA 2002 while offering internet banking.

Annex-II

Internet Banking - Security Features:

1. RRBs need to ensure suitable security measures for their web Applications and take reasonable mitigating measures against various web security risks.

2. Web Applications should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage leading to compromise in the integrity of the data. Critical web Applications should enforce at least SSL v3 or Extended Validation –SSL / TLS 1.0 128 bit encryption level for all online activity.

3. Re-establishment of any session after interruption should require normal user identification, authentication, and authorization. Moreover, strong server side validation should be enabled.

4. RRBs need to follow a defense-in-depth strategy by applying robust security measures across various technology layers.

Authentication practices for internet banking:

1. Authentication methodologies involve three basic ‘factors’:

- Something the user knows (e.g., password, PIN);

- Something the user has (e.g., ATM card, smart card); and

- Something the user is (e.g., biometric characteristic, such as a fingerprint).

2. Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The principal objectives of two-factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in internet banking by combating various cyber attack mechanisms like phishing, keylogging, spyware/malware and other internet based frauds targeted at banks and their customers.

Implementation of two-factor authentication and other security measures for internet banking:

a. In view of the proliferation of cyber-attacks and their potential consequences, banks should implement two-factor authentication for fund transfers through internet banking.

b. The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution’s Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/commercial); the customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information and the volume of transactions involved.

c. Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems.

d. There is a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. For carrying out critical transactions like fund transfers, the banks, at the least, need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like (a) a digital signature (through a token containing digital certificate and associated private key, preferably for corporate customers) or (b) One Time Password (OTP) / dynamic access code through various modes (like SMS over mobile phones or hardware token).

e. To enhance online processing security, confirmatory second channel procedures (like telephone, SMS, e-mail, etc.) should be applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, banks should take into account their efficacy and differing customer preferences for additional online protection.

f. Based on mutual authentication protocols, customers could also authenticate the bank’s web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the Secure Sockets Layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. These are special SSL Certificates that work with high security web browsers to clearly identify a website's organizational identity. It should, however, be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.

g. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.

h. Changes in mobile phone number may be done through request from a branch only.

i. Virtual keyboard should be implemented.

j. A cooling period for beneficiary addition and SMS / e-mail alerts may be introduced when new beneficiaries are added.

k. Customers should be advised to adopt various good security precautions and practices in protecting their personal computer and to avoid conducting financial transactions from public or internet café computers.

l. Risk-based transaction monitoring or surveillance process needs to be considered as an adjunct.

m. An online session would need to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

n. By definition, true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute a true multifactor authentication.

o. As an integral part of the two factor authentication architecture, banks should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack.

p. The banks should also consider, and if deemed appropriate, implement the following control and security measures to minimize exposure to man-in-the middle attacks:

(i) Specific OTPs for adding new payees: Each new payee should be authorized by the customer based on an OTP from a second channel which also shows payee details or the customer’s handwritten signature from a manual procedure which is verified by the bank.

(ii) Individual OTPs for value transactions (payments and fund transfers): Each value transaction or an approved list of value transactions above a certain monetary threshold determined by the customer should require a new OTP.

(iii) OTP time window: Challenge-based and time-based OTPs provide strong security because their period of validity is controlled entirely by the bank and does not depend on user behavior. It is recommended that banks should not allow the OTP time window to exceed 100 seconds on either side of the server time since the smaller the time window, the lower the risk of OTP misuse.

(iv) Payment and fund transfer security: Digital signatures and Key-based Message Authentication Codes (KMAC) for payment or fund transfer transactions could be considered for detection of unauthorized modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him, which means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.

(v) In internet banking scenario, there is very little scope for banks to act on stop-payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.

(vi) The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. The rights and liabilities of customers availing of internet banking services need to be clearly explained to customers opting for internet banking. Considering the banking practice and rights enjoyed by customers in traditional banking, the 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 internet banking should insure themselves against such risks.

(vii) Hyperlinks from banks' websites often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business unrelated to banking. Hyperlinks from banks' websites should be confined to only those portals with which they have a payment arrangement. Hyperlinks to banks' websites from other portals are normally meant for passing on information relating to purchases made by banks' customers in the portal. Banks must follow recommended security precautions while dealing with requests received from other websites relating to customers' purchases.

(viii) **Second channel notification / confirmation:** The bank should notify the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.

(ix) **SSL server certificate warning:** Internet banking customers should be made aware of and shown how to react to SSL or EV-SSL certificate warning.

(x) Banks should put in place risk-based transaction monitoring and surveillance process. Study of customer transaction behaviour pattern and stopping irregular transaction or obtaining prior confirmation from customers for outlier transactions may be incorporated in the software.