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

RBI/2011-12/202

UBD.BPD.(SCB)Cir No. 1/09.18.300/2011-12 September 26, 2011

The Chief Executive Officers
All Scheduled Primary (Urban) Co-operative Banks

Madam / Dear Sir,

Internet Banking for Customers of UCBs

As announced in the Monetary Policy Statement 2011-12, [para 102 - appended], it has been decided to permit scheduled UCBs satisfying certain criteria to provide internet banking facility to their customers. Accordingly, scheduled UCBs having minimum networth of Rs. 100 crore, CRAR of at least 10%, net NPA less than 5% and have earned net profit continuously in the last three financial years are eligible to offer internet banking facility to their customers. Eligible UCBs, desirous of offering internet banking facility, may, with the approval of their Board, frame a policy on internet banking in accordance with the Guidelines given in the Annex 1 and 2 and approach the Regional Office concerned of Reserve Bank of India for permission before offering such facility to their customers.

2. The application for permission to undertake internet banking should be accompanied by an internet banking policy as approved by the Board of Directors and the policy should fit into the overall Information Technology (IT) and Information System (IS) policy of the bank. The application should also be accompanied by a cost benefit analysis, details of operational arrangements like technology adopted, business partners, if any, and systems and controls the bank proposes to adopt for

शहरी बैंक विभाग, केन्द्रीय कार्यालय, गारमेंट हाउस, पहली मंजिल, वरली, मुंबई - 400 018
फोन: 022 - 2493 9930 - 49, फैक्स: 022 - 2497 4030 / 2492 0231, ई मेल: rbiubdco@rbi.org.in
Urban Banks Department, Central Office, 1 Floor, Garment House, Worli, Mumbai - 18
Phone: 022 - 2493 9930 - 49, Fax: 022 - 2497 4030 / 2492 0231, Email: rbiubdco@rbi.org.in

managing risks. The bank should also submit a certificate from a Certified Information System Auditor to the effect that the IT and IS policy requirements prescribed in the Guidelines attached to this Circular have been adhered to by the bank.

3. Please acknowledge receipt of this Circular to the Regional Office concerned.

Yours faithfully

(A. Udgata)
Chief General Manager- in – Charge

Encl: 11

Annex - 1

Guidelines for offering Internet Banking to Customers of UCBs

Scheduled UCBs intending to offer internet banking facility to their customers should frame a policy for Internet Banking with the approval of the Board. The said policy should adequately address Technology and Security Standards as also the Legal Issues. The UCBs should also have sound internal control systems in place and take into account the operational risk as also give adequate disclosure to its customers on the risk, responsibilities and liabilities of the customers before offering internet banking.

I. Technology and Security Standards:

a. UCBs should have an 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. UCBs should designate a network and database administrator with clearly defined roles.

c. Logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. should be in place.

d. UCBs should ensure that there is no direct connection between the Internet and the bank's system.

e. UCBs should have effective safeguards to prevent intrusions into the network.

f. It is also recommended that 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 the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The banks 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 undertake 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. UCBs 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 given 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 of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form.

l. Security infrastructure should be properly tested before using the systems and applications for normal operations. UCBs should periodically upgrade the systems to newer versions which give better security and control.

In addition to the above, security features as described in **Annex 2** should be taken into account while offering internet banking to customers.

II. Legal Issues

a. 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 customer opting for internet banking. Therefore,

even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction, verification of the identity of the customer and adherence to KYC guidelines.

b. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. The prescriptions of the the Information Technology Act, 2000, and other legal provisions need to be scrupulously adhered to while offering internet banking.

c. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts. 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 UCBs should, therefore, institute adequate risk control measures to manage such risks.

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

e. 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, UCBs' 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.

III. Internal Control System

UCBs should develop sound internal control systems before offering internet banking. This would include internal inspection / audit of system and procedures related to internet banking as also ensuring that safeguards are in place to protect the integrity of data, customer confidentiality and security

of the data. UCBs may also consider prescribing suitable monetary limits for customers on transactions put through internet banking. The system of internal control should cover the following:

a. **Role and Responsibilities / Organisational structure:** The Board of Directors and senior management are responsible for ensuring that the system of internal control operates effectively. The 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 the UCB.

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 UCBs 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.

IV. Other Issues and Disclosures:

The existing regulatory framework over 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 only include local currency products.

c. UCBs 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.

e. 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 request received from other websites, relating to customers' purchases.

Annex - 2

Internet Banking - Security Features:

1. UCBs 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. UCBs 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:

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

2. 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.

3. 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.

4. 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 UCBs, 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 the corporate customers) or (b) One Time Password (OTP) / dynamic access code through various modes (like SMS over mobile phones or hardware token).

5. To enhance online processing security, confirmatory second channel procedures(like telephony, SMS, email 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, UCBs should take into account their efficacy and differing customer preferences for additional online protection.

6. 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 Web site'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.

7. 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.

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

9. Virtual keyboard should be implemented.

10. A cooling period for beneficiary addition and SMS and E-mail alerts, may be introduced when new beneficiaries are added.

11. 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.

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

13. 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.

14. 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.

15. As an integral part of the two factor authentication architecture, UCBs 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. The banks should also consider, and if deemed appropriate, implement the following control and security measures to minimise exposure to man-in-the middle attacks:

a. 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.

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

c. 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 the UCBs 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.

d. Payment and fund transfer security: Digital signatures and Key-based Message Authentication Codes (KMAC) for payment or fund transfer transactions could be considered for the 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.

e. 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.

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

Monetary Policy 2011-12 - Extract of Para 102

102. With increasing expectation of customers of UCBs for better products and services on par with commercial banks, the opening up of internet banking channel to UCBs will enable them to retain their customer base. It is, therefore, proposed:

- to permit scheduled UCBs satisfying certain criteria to provide internet banking facility to their customers.