Annex-I

Guidelines on Internet Banking facility to Customers of Cooperative banks

Licensed StCBs, DCCBs and UCBs 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 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.

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

I. Technology and Security Standards:

a. Cooperative banks 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 banks 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 banks should ensure that there is no direct connection between the Internet and the bank's system.

e. The banks 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 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 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 banks 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 banks 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 / UBD.No.Admn.46b/17:36:00/97-98 dated March 30, 1998 and circular 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.

o. In the case of StCBs/DCCBs, 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 banks should, therefore, have in place adequate risk control measures to manage such risks.

III. Internal Control System

The banks 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 banks 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 Cooperative banks 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 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 include only local currency products.

c. Cooperative banks 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.