Internet Banking in India – Guidelines

DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01

June 14, 2001

All Scheduled Commercial Banks

Dear Sir,

Internet Banking in India – Guidelines

You may be aware that Reserve Bank of India had set up a 'Working Group on Internet Banking' to examine different aspects of Internet Banking (I-banking). The Group had focussed on three major areas of I-banking, i.e, (i) technology and security issues, (ii) legal issues and (iii) regulatory and supervisory issues. A copy of the Group's report is enclosed. RBI has accepted the recommendations of the Group to be implemented in a phased manner. Accordingly, the following guidelines are issued for implementation by banks. Banks are also advised that they may be guided by the original report, for a detailed guidance on different issues.

I. Technology and Security Standards:

a. Banks should designate a network and database administrator with clearly defined roles as indicated in the Group's report. (Para 6.2.4)

b. Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems. (Para 6.3.10, 6.4.1)

c. Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies. (Para 6.4.2)

d. At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank's system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert. (Para 6.4.3)

e. All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server. (Para 6.4.4)

f. PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. However, as it is not yet commonly available, banks should use the following alternative system during the transition, until the PKI is put in place:

   1. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the banks themselves using a Certificate Server.
   2. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself. (Para 6.4.5)

g. It is also recommended that all unnecessary services on the application server such as FTP (File Transfer Protocol), telnet should be disabled. The application server should be isolated from the e-mail server. (Para 6.4.6)

h. All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be reported and follow up action taken should be kept in mind while framing future policy. 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. They should educate their security personnel and also the end-users on a continuous basis. (Para 6.4.7, 6.4.11, 6.4.12)

i. 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 DDoS (Distributed Denial of Service) & DoS (Denial of Service) 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’). (Para 6.4.8)

j. 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. (Para 6.4.9)

k. 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 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. (Para 6.4.10)

l. 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. (Para 6.4.13)

m. Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control. (Para 6.4.15)

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 prospective customer. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer. (Para 7.2.1)

b. From a legal perspective, 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, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk. (Para 7.3.1)

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/ other technological failures. The banks should, therefore, institute adequate risk control measures to manage such risks. (Para 7.5.1-7.5.4)

d. In Internet banking scenario there is very little scope for the 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. (Para 7.6.1)

e. 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 Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, 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. (Para 7.11.1)

III. Regulatory and Supervisory Issues:

As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:

1. Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.

2. The products should be restricted to account holders only and should not be offered in other jurisdictions.
3. The services should only include local currency products.
4. The 'in-out' scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the 'out-in' scenario where Indian residents are offered banking services by banks operating in cross-border jurisdictions are generally not permitted and this approach will apply to Internet banking also. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.
5. Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor.

Given the regulatory approach as above, banks are advised to follow the following instructions:

a. All banks, who propose to offer transactional services on the Internet should obtain prior approval from RBI. Bank's application for such permission should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners, third party service providers and systems and control procedures the bank proposes to adopt for managing risks. The bank should also submit a security policy covering recommendations made in this circular and a certificate from an independent auditor that the minimum requirements prescribed have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services / products offered by them. (Para 8.4.1, 8.4.2)

b. Banks will report to RBI every breach or failure of security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks. (Para 8.4.3)

c. 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 will equally apply to Internet banking. The RBI as supervisor will cover the entire risks associated with electronic banking as a part of its regular inspections of banks. (Para 8.4.4, 8.4.5)

d. Banks should develop outsourcing guidelines to manage risks arising out of third party service providers, such as, disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks' systems and misutilizing the same, etc., effectively. (Para 8.4.7)

e. With the increasing popularity of e-commerce, it has become necessary to set up 'Inter-bank Payment Gateways' for settlement of such transactions. The protocol for transactions between the customer, the bank and the portal and the framework for setting up of payment gateways as recommended by the Group should be adopted. (Para 8.4.7, 8.4.9.1 – 8.4.9.5)

f. Only institutions who are members of the cheque clearing system in the country will be permitted to participate in Inter-bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intra-bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway. (Para 8.4.7)

g. Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as far as possible, in real time. (Para 8.4.7)

h. Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL / 128 bit encryption must be used as minimum level of security. Reserve Bank may get the security of the entire infrastructure both at the payment gateway's end and the participating institutions' end certified prior to making the facility available for customers use. (Para 8.4.7)

i. Bilateral contracts between the payee and payee's bank, the participating banks and service provider and the banks themselves will form the legal basis for such transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law. (Para 8.4.7)

j. Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template. The banks should also provide their latest published financial results over the net. (Para 8.4.8)

k. 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 a banks' websites should be confined to only those portals with which they have a payment arrangement or sites of their subsidiaries or principals. 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 the minimum recommended security precautions while dealing with request received from other websites, relating to customers' purchases. (Para 8.4.9)

2. The Reserve Bank of India have decided that the Group's recommendations as detailed in this circulars should be adopted by all banks offering Internet banking services, with immediate effect. Even though the recommendations have been made in the context of Internet banking, these are applicable, in general, to all forms of electronic banking and banks offering any form of electronic banking should adopt the same to the extent relevant.

3. All banks offering Internet banking are advised to make a review of their systems in the light of this circular and report to Reserve Bank the types of services offered, extent of their compliance with the recommendations, deviations and their proposal indicating a time frame for compliance. The first such report must reach us within one month from the date of this circular. Banks not offering any kind of I-banking may submit a 'nil' report.

4. Banks who are already offering any kind of transactional service are advised to report, in addition to those mentioned in paragraph above, their business models with projections of cost / benefits etc. and seek our post-facto approval.

5. Please acknowledge receipt.

Yours faithfully,

(M. R. Srinivasan)
Chief General Manager-in-Charge

Encls: As above