Annex-II

Internet Banking - Security Features:

1. Cooperative banks 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. Cooperative banks 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.