

APPENDIX B

INTERNET AND WIRELESS BANKING SECURITY MEASURES

1. Network controls

- Implement adequate security measures on the internal networks and network connections to public network or remote parties. Segregate internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment.
- Properly design and configure the servers and firewalls used for the e-banking services either internet-based or delivered through wireless communication networks (e.g., install firewalls between internal and external networks as well as between geographically separate sites).
- Deploy strong and stringent authentication and controls especially in remote access or wireless access to the internal network.
- Implement anti-virus software, network scanners and analyzers, intrusion detectors and security alert as well as conduct regular system and data integrity checks.
- Maintain access security logs and audit trails. These should be analyzed for suspicious traffic and/or intrusion attempts.
- Ensure that wireless software for wireless communication network includes appropriate audit capabilities (e.g., recording dropped transactions).
- Develop built-in redundancies for single points of failure which can bring down the entire network.

2. Operating Systems Controls

- Harden operating systems by configuring system software and firewall to the highest security settings consistent with the level of protection required, keeping abreast of enhancements, updates and patches recommended by system vendors.
- Change all default passwords for new systems immediately upon installation as they provide the most common means for intruders to break into systems.

3. Encryption

- Implement encryption technologies that are appropriate to the sensitivity and importance of data to protect confidentiality of information while it is stored or in passage over external and internal networks.
- Choose encryption technologies that make use of internationally recognised cryptographic algorithms where the strengths of the algorithms have been subjected to extensive tests.
- Apply strong "end-to-end" encryption to the transmission of highly sensitive data (e.g., customer passwords) so that the data are encrypted all the way between customers' devices and bank's internal systems for processing the data. This would ensure that highly sensitive data would not be compromised even if the banks' web servers or internal networks were penetrated.

4. Website and Mobile Banking Authentication

- Authenticate official website to protect bank customers from spoofed or faked websites. Banks should determine what authentication technique to use to provide protection against these attacks.
- For wireless applications, adopt authentication protocols that are separate and distinct from those provided by the wireless network operator.

5. Physical Security

- House all critical or sensitive computers and network equipment in physically secure locations (e.g., away from environmental hazards, unauthorized entry and public disclosure, etc.).
- Implement physical security measures such as security barriers (e.g., external walls, windows); entry controls (e.g., biometric door locks, manual or electronic logging, security guards) and physical protection facilities/devices (e.g., water and fire detectors, uninterruptible power supply (UPS), etc.) to prevent unauthorized physical access, damage to and interference with the e-banking services.

6. Development and Acquisition

- Separate physical/logical environments for systems development, testing and production.
- Provide separate environments for the development, testing, staging and production of internet facing web-based applications; connect only the production environment to the internet.

7. IT Personnel Training

- Provide appropriate and updated training to IT personnel on network, application and security risks and controls so that they understand and can respond to potential security threats.

8. Service Providers

- Perform due diligence regularly to evaluate the ability of the service providers (e.g., internet service provider, telecommunication provider) to maintain an adequate level of security and to keep abreast of changing technology.
- Ensure that the contractual agreements with the service providers have clearly defined security responsibilities.

9. Independent Audit, Vulnerability Test and Penetration Testing

- Conduct regular audit to assess the adequacy and effectiveness of the risk management process and the attendant controls and security measures.
- Perform vulnerability test or assessment to evaluate the information security policies, internal controls and procedures, as well as system and network security of the bank. Assessment should also include latest technological developments and security threats, industry standards and sound practices.
- Conduct penetration testing at least annually.
- The audit and tests should be conducted by security professionals or internal auditors who are independent in the development, implementation or operation of the e-banking services, and have the required skills to perform the evaluation.
- For e-banking services provided by an outside vendor or service provider, ensure that the above tests and audit are performed and the bank is provided with the results and actions taken on system security weaknesses.

10. Incident Response

- Establish an incident management and response plan and test the predetermined action plan relating to security incidents.