State of Washington

DEPARTMENT OF FINANCIAL INSTITUTIONS

Division of Consumer Services

P.O. Box 41200 ● Olympia, Washington 98504-1200

Telephone (360) 902-8703 ● TDD (360) 664-8126 ● FAX (360) 704-6945 ● http://www.dfi.wa.gov/cs

Information Security in Consumer Services Companies

The Gramm-Leach Bliley Act (GLBA) was enacted in order to establish standards for protecting the security and confidentiality of customer non-public personal information at financial institutions. The Safeguards Rule, which implements sections of the GLBA for financial institutions under the jurisdiction of the Federal Trade Commission (FTC), sets standards for implementing an information security program. An adequate Information Security Program must contain the following five elements:

- One or more employees designated to coordinate the information security program
- A risk assessment conducted to identify and assess possible threats to customer information for each area of the company's operations
- Safeguards designed to mitigate threats and to ensure the confidentiality, integrity and availability of information assets
- All third party service providers who handle customer information maintain the appropriate safeguards which mitigate threats
- Periodically review and assess the effectiveness of the information security program

There is real potential for harm from unsecure information for financial institutions and the consumers who rely on their services. Laws require financial institutions to create a comprehensive information security program, but there are also many business incentives for maintaining information security. For instance, your customers have an expectation that their non-public information will be protected and held in confidence by your company. Additionally, it is vital for your business that information be stored securely so that the information can be trusted as reliable and accurate. Ensuring that information be available for access when it is needed by those who require it is also essential for business.

Below is list of fundamental information security elements.

1. **All computers have anti-virus and anti-spyware software installed and regularly updated**.
   Anti-virus and anti-spyware software should be set to automatically check for updates and conduct full system scans regularly.

2. **All computers which have an Internet connection are secured by a hardware firewall in the form of a wireless access point/router**.

3. **All computers have a software firewall installed and regularly updated.**
   Most operating systems (such as Windows or Mac OS) have a software firewall provided which can be activated in the system settings.

4. **All operating systems and applications are regularly patched, updated and functioning properly.**
   Most operating systems and applications have the option to check for updates and patches automatically.

5. **All information stored electronically for business purposes is backed up regularly.**

6. **All computers have their access restricted only to authorized persons.**
   All computers should be set to automatically lock-out when not in use.

7. **All wireless access points/routers and networks are kept secure. All information traveling outside of the secure network is properly encrypted.**
   All wireless access points/routers should implement WiFi Protected Access 2 (WPA-2) using the Advanced Encryption Standard (AES). Wired-Equivalent Privacy (WEP) is not considered secure.

8. **All employees who have access to computers are properly trained to ensure information security is maintained.**

9. **All employees who have access to computers and network components have individual accounts, including separate log-in identities and passwords.**

10. **User access and privileges should be limited to the immediate job functions of the employee.**