GLB Act Safeguards Rule
Recomended Practices

Employee Management and Training

- Background and reference checks prior to hiring employees who will have access to customer infomraiton.
- Requesting employees to sign an agreement to follow compnay security and confidentialtiy standards.
- Limiting employee access to customer infomraiton.
- Controlling acess to information through the use of strong passwords that change on a regular basis.
- Develop policies for employees that telecommute and require employees who use personal computers to access or store customer information to use protections against viruis, spyware and unauthorized intrusions.
- Utilizing password activated screensavers to lock employee cmputers after a period of inactivity.
- Train employees to take basic steps to maintain the security of customer information.
- Develop policies for appropriate use and protection of laptops, cell phones and other devices.
- Impose disciplinary measures for security policy violations
- Prevent terminated employees from accessing customer informaiton by immediatley deactivnig their usernames and passwords.

Information Systems

- Know where sensitive cusomter information is stored and stored securely.
- Ensure that servers and computers are only accesable suing a strong password and are kept in a physically secure area.
- Maintain secure backup records and keep archived data secure by storing it offline and in a physically secure area.
- Secure transmission of customer infomration via SSL or other secure connection.
- Encrypy customer data if transmitted by email or the internet.
- If data is collected online directly from customers, automattically secure data transmissions.
- Maintain a careful inventory of your company's computers and any other equipment used to store customer information.
- Dispose of customer infomraiotn consisent with the FTC Dispostal Rule.

Managing Attacks and System Failures

- Check with software vendors to install patches and resolve security vulnerabilities.
- Use anti-virus and anti-spyware software that updates automatically.
- Maintain up to date firewalls.
- Monitor both in and out bound transfers of information for signs of a compromise or unauthorized users.
- Use appropriate audit or oversight procedures to detect theft or improper disclosure of customer information. Take steps to preserve the security confidentiality and integrity of customer information in the event of a technological failure.
- Notify customers and relevant agencies promptly if personal information is subject to loss, damage or unauthorized access.
- Preserve and review files or programs that may reveal how the breach occurred.