GLB Act Safeguards Rule
Recommended Practices

Employee Management and Training

• Background and reference checks prior to hiring employees who will have access to customer information.
• Requesting employees to sign an agreement to follow company security and confidentiality standards.
• Limiting employee access to customer information.
• Requesting employees to follow company security and confidentiality standards.
• Controlling access 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 viruses, spyware and unauthorized intrusions.
• Utilizing password-activated screensavers to lock employee computers 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 information by immediately deactivating their usernames and passwords.

Information Systems

• Know where sensitive customer information is stored and stored securely.
• Ensure that servers and computers are only accessible using 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 information via SSL or other secure connection.
• Encrypt customer data if transmitted by email or the internet.
• If data is collected online directly from customers, automatically secure data transmissions.
• Maintain a careful inventory of your company’s computers and any other equipment used to store customer information.
• Dispose of customer information consistent with the FTC Disposal 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 inbound and outbound 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.

This guide is provided for informational purposes only. For updated information and a complete listing of the GLBA Act, please visit the Federal Trade Commission website.