

What is the Gramm-Leach-Bliley Act?

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLB Act), protects the privacy of consumer information held by financial institutions and requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. The Act also provides consumers with the right to limit some sharing of their information.

Who is affected?

The GLB Act applies to almost any business that is involved in providing financial products or services to consumers. These "financial institutions" include check-cashing businesses, mortgage brokers, banks, insurance companies, real estate appraisers, tax preparation businesses and accountants, ATM operators and others.

Under the law, financial institutions are required to protect information collected about individuals. They must develop their own safeguards and are responsible for ensuring that their affiliates and service providers also safeguard consumer information.

What does the GLB Act have to do with information management?

Under the GLB Act, the Safeguards Rule, requires financial institutions to have a security plan to protect personal consumer information. The plan must address information systems, including how personal information is stored and destroyed.

The Safeguard Rule is introduced under Section 501(b) of the GLB Act. Additional detail is provided in section 314.4 of the rule:

314.4 Elements – In order to develop, implement, and maintain your information security program, you shall:
(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

What do companies have to do to comply with GLB Act?

Among other things, financial institutions must develop a written security plan appropriate to the size and type of business. The Federal Trade Commission, the government agency responsible for administering the GLB Act, recommends appropriate document storage and destruction protocols. For example, storing records in a secure area, accessible only to authorized employees and shredding customer information recorded on paper.

Failure to comply with the GLB Act's Safeguard Rule may result in an enforcement action by the Federal Trade Commission (FTC). Failure to comply with an FTC enforcement order can result in civil penalties of up to \$11,000 per violation.

How can we help?

We recommend discussing our customer's security plans with them to ensure we understand what is required and where we can help. For example, Securit's document destruction technology assures companies that their customer information is being destroyed in a secure manner. Employees place materials to be shredded in locked boxes which are picked up and shredded onsite. Securit Certificate of Destruction is a company's record of the secure destruction process. For peace of mind, contact Securit today at 1 800 697-4733.

For more information:

Federal Trade Commission – www.ftc.gov/privacy.

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2005

