

GRAMM-LEACH-BLILEY ACT (“GLB”) An Overview

Who is covered?

Financial Institutions.

What is a Financial Institution?

A financial institution is an entity that regularly provides financial products (brokerage, credit or loans) or financial services (making, acquiring, brokering, collecting, or servicing loans) to consumers.

Who is a Consumer?

A consumer is a person who has obtained a financial product or service from a financial institution, such as applying for credit or providing information to obtain a loan.

Is the University a Financial Institution?

Yes, because it regularly provides financial products and services, such as making Federal Perkins Loans.

What is the purpose of GLB?

To safeguard and to protect the privacy of non-public personal information.

What is Nonpublic Personal Information?

Nonpublic personal information is, most notably, personally identifiable financial information (“PIFI”).

What is PIFI?

PIFI is any information: (i) provided by a consumer to obtain credit, a loan or other financial product or service; (ii) about a consumer resulting from a financial product or service transaction; or (iii) obtained about a consumer in connection with providing a financial product or service.

Are Universities subject to the privacy provisions of the GLB?

Universities are deemed in compliance with the privacy provisions of the GLB if they are in compliance with FERPA (no disclosure of personally identifiable student record information without written consent of the student).

Are Universities subject to the safeguarding provisions of the GLB?

Yes.

What do the safeguarding provisions require?

Standards for safeguarding customer information:

Definitions.

“Information security program” means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Requirements.

Develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the institutions size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue. Such safeguards shall include the following elements.

Elements:

- (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 (vendor’s contracts), 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) Periodically evaluate and adjust your information security program in light of the results of the testing and monitoring mentioned above; 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.

Objectives.

The objectives of such information security program are to:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Effective date.

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the service provider requirements above, even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

Which offices within the University are affected by GLB?

Those offices that access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle PIFI.

Which vendor's contracts must be subject to contractual terms for safeguarding PIFI?

All contracts with vendors who, as an agent of the University, access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle PIFI.

<http://security.arizona.edu/glba>