



AMERICAN UNIVERSITY
WASHINGTON, D.C.

GRAMM-LEACH-BLILEY FACT SHEET

- **What is the Gramm-Leach-Bliley Act?**

The Gramm-Leach-Bliley Act (GLB) requires financial institutions to ensure the privacy and security of the non-public personal information of customers of financial services and products. In order to implement the mandate of GLB, the FTC issued two sets of regulations, the Privacy Rule and Safeguards Rule.

- **What is non-public personal information or Customer Information?**

A customer's non-public personal information is any data which a financial institution collects in connection with its provision of a financial service or product. Examples include the customer's name, address, and phone number; date of birth; bank and credit card account number and balance; credit history and rating; income and tax return information; and social security numbers.

- **Are universities classified as financial institutions?**

The GLB considers universities as financial institutions because they are engaged in financial activities such as lending funds to students/staff, provide financial aid services, and collecting debts.

- **How do universities satisfy the GLB Privacy Rule?**

The first set of regulations the FTC adopted under GLB relates to the privacy of Customer Information. These regulations have been in effect for several years, and most people have encountered the results of GLB's privacy protections in the form of privacy practice notices from their banks, accountants, and other businesses from which they receive financial services. Universities which comply with FERPA were exempted from the Privacy Rule.

- **How do universities satisfy the GLB Safeguard Rule?**

The second set of regulations, Safeguards Rule, requires financial institutions to protect the security of non-public personal information. These regulations became effective May 23, 2003 and there is no exemption for higher education institutions. Thus, universities must implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of Customer Information. The safeguards may be tailored to the size and complexity of the institution and the nature and scope of its activities.

- **What are the goals of the GLB information security program?**

The information security program must be designed to protect customer information/records by:

- (1) Ensuring the security and confidentiality of the information;
- (2) Protecting against any anticipated threats or hazards to the security or integrity of such records;

and

- (3) Protecting against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

- **What are the requirements of an information security program?**

- (1) Designate employee/employees to implement the plan;
- (2) Perform operational assessment to identify foreseeable internal and external risks to the security of Customer Information;
- (3) Design and implement information administrative, physical, and technical safeguards to control the risks;
- (4) Take reasonable steps to assure contracted service providers have sufficient security procedures and require them, by contract, to implement and maintain such safeguards; and

(5) Must monitor, evaluate and adjust its information security program periodically to address changes.

- **What are the important considerations in designing an information security program?**

The appropriate measures for each institution will vary depending on the institution's size and complexity.

- (1) employee training and management (e.g. checking references, confidentiality agreement);
- (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.