

Gramm-Leach-Bliley Act: Implementation of the Safeguards Rule

Purdue University

IT-Security and Policy

(Revised November 2005)

Objectives for GLBA Training

- Understand the applicability of GLBA and the Federal Trade Commission's Safeguards Rule
- Understand what information is protected and why
- Understand different types of safeguards
- Understand the role of departments and IT in safeguarding information
- Understand the requirements for ongoing training on safeguards
- Provide resources for additional questions

What is GLBA?

- The Gramm Leach Bliley Act (GLBA) is a comprehensive, federal law affecting financial institutions. The law requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information.
- The GLBA is composed of several parts, including the Privacy Rule (16 CFR 313) and the Safeguards Rule (16 CFR 314).

GLBA Compliance with the Privacy Rule

The Federal Trade Commission (FTC) has officially stated that any college or university that complies with the Federal Educational Rights and Privacy Act (FERPA) (20 U.S.C. 1232g) and that is also a financial institution subject to the requirements of GLBA shall be deemed to be in compliance with GLBA's privacy rules if it is in compliance with FERPA. (16 CFR 313.1)

The FTC has not made a similar exception for an institution of higher education with respect to the Safeguards Rule.

- Purdue must comply with the Safeguards Rule.

Why does the GLBA Safeguards Rule apply to Purdue?

- Purdue significantly engages in student loan making and provides other financial services. As such, Purdue falls within the definition of “financial institution” under the GLBA and must comply with the laws requirements.
- “Financial Institution” means any institution the business of which is engaging in financial activities.

Examples of Purdue University Financial Products and Services Covered Under GLBA:

- Student loans, including receiving application information, and the making and servicing of such loans
- Financial advisory services (very limited at Purdue)
- Collection of delinquent loans
- Check cashing services
- Tax planning (very limited at Purdue)
- Obtaining information from a consumer report
- Career counseling services for those seeking employment in finance, accounting or auditing

Examples of Other Financial Products and Services Covered Under GLBA:

- Other kinds of financial products and services are covered by GLBA that are not currently offered by Purdue University. However, as business processes change and new academic programs and employee benefits are offered, the full scope of covered activities needs to be kept in mind. Examples include:
 - Investment advisory services
 - Credit counseling services
 - Tax preparation
 - Sale of money orders, savings bonds, or traveler's checks
 - Travel agency services provided in connection with financial services
 - Real estate settlement services
 - Money wiring services
 - Issuing credit cards or long term payment plans involving interest charges
 - Personal property and real estate appraisals
 - Services provided by a principal, broker or agent with respect to life, health, liability, or disability insurance products
 - Providing or issuing annuities

Why Comply with the Safeguards Rule?

“Adequately securing customer information is not only the law – it makes good business sense. When you show customers that you care about the security of their personal information, you increase the level of their confidence in your institution. Poorly-managed customer data can lead to identity theft. Identity theft occurs when someone steals a customer’s personal identifying information to open new charge accounts, order merchandise, or borrow money.”

FTC Facts for Business (www.FTC.gov) *Financial Institutions and Customer Data: Complying with the Safeguards Rule*

- *Customer Information* is any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.

Customer Information (cont'd)

- GLBA applies to customer information obtained in a variety of situations, including:
 - Information provided to obtain a financial product or service;
 - Information about a customer resulting from any transaction involving a financial product or service between the institution and a customer;
 - Information otherwise obtained about a customer in connection with providing a financial product or service to the customer.

GLBA Definitions (Continued)

Non-Public Personal Information means personally identifiable financial information that is:

1. Provided by a consumer to a financial institution;
2. Resulting from any transaction with the consumer or any service performed for the consumer; or
3. Otherwise obtained by the financial institution.

The term also includes any list, description, or other grouping of consumers and publicly available information pertaining to them that is derived using any personally identifiable financial information that is not publicly available.

Examples of Nonpublic Personal Information (NPI) Include:

- Social Security Number (SSN)
- Financial account numbers
- Credit card numbers
- Date of birth
- Name, address, and phone numbers when collected with Financial data
- Details of any financial transactions

The objectives of the GLBA Safeguards Rule 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.

What is the FTC Safeguards Rule?

- The Safeguards Rule requires all financial institutions to develop an information security program to protect customer information. This program must include:
 - Designation of staff to coordinate the safeguards program
 - Identification and assessment of risks in each relevant area of the operation and an evaluation of the effectiveness of current safeguards
 - Design and implementation of a safeguards program including regular monitoring and followup
 - Selection of appropriate service providers including inclusion of contract language designed to protect customer information handled by service providers
 - Evaluation and adjustment of the program in light of relevant circumstances and changes in the business.

When a Purdue department implements safeguards to protect the security, confidentiality, and integrity of customer information, there are three types of safeguards that must be considered:

1. Administrative Safeguards
2. Technical Safeguards; and
3. Physical Safeguards.

A department must assume responsibility for assuring adequate safeguards are in place within its area of responsibility.

- Administrative safeguards are generally within the direct control of a department and include:
 - Reference checks for potential employees
 - Confidentiality agreements that include standards for handling customer information
 - Training employees on basic steps they must take to protect customer information (see detail later slide)
 - Assure employees are knowledgeable about applicable policies and expectations
 - Limit access to customer information to employees who have a business need to see it
 - Impose disciplinary measures where appropriate

Physical Safeguards

- Physical safeguards are also generally within a department's control and include:
 - Basic Steps –
 - » Locking rooms and file cabinets where customer information is kept
 - » Using password activated screensavers
 - » Using strong passwords
 - » Changing passwords periodically and not writing them down
 - » Encrypting sensitive customer information transmitted electronically
 - » Referring calls or requests for customer information to staff trained to respond to such requests
 - » Being alert to fraudulent attempts to obtain customer information and reporting these to management for referral to appropriate law enforcement agencies

Physical Safeguards (continued)

- Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods
- Store records in a secure area and limit access to authorized employees
- Dispose of customer information appropriately:
 - » Designate a trained staff member to supervise the disposal of records containing customer personal information
 - » Shred or recycle customer information recorded on paper and store it in a secure area until the recycling service picks it up
 - » Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information
 - » Promptly dispose of outdated customer information within record retention policies

- Technical safeguards are generally the responsibility of IT or departmental/Zone computing staff. Departments, however, should be knowledgeable regarding how their digital customer information is safeguarded. If additional controls are warranted, departments should work with IT or Zone staff to improve safeguards.
- Departments are also responsible for alerting IT and Zone staff to the existence of customer information on networks

Examples of Technical Safeguards

- Technical safeguards include:
 - » Storing electronic customer information on a secure server that is accessible only with a password - or has other security protections - and is kept in a physically-secure area
 - » Avoiding storage of customer information on machines with an Internet connection
 - » Maintaining secure backup media and securing archived data
 - » Using anti-virus software that updates automatically
 - » Obtaining and installing patches that resolve software vulnerabilities
 - » Following written contingency plans to address breaches of safeguards
 - » Maintaining up-to-date firewalls particularly if the institution uses broadband Internet access or allows staff to connect to the network from home
 - » Providing central management of security tools and keep employees informed of security risks and breaches

Guidelines for Providing Secure Data Transmission

- if you collect credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection so that the information is encrypted in transit;
- if you collect information directly from consumers, make secure transmission automatic. Caution consumers against transmitting sensitive data, like account numbers, via electronic mail; and
- if you must transmit sensitive data by electronic mail, ensure that such messages are password protected so that only authorized employees have access.

- Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures.
- Requires policies and procedures to deal with these failures.

Role of IT Security & Policy in GLBA compliance

- Risk Assessments
- Guidelines for secure computer data
- Educational Materials
- Providing security tools and software
- Providing support for security issues
- Security event response

- The FTC may bring an administrative enforcement action against any financial institution for non-compliance with the Safeguards Rules.
- Penalties for violating Safeguards Rule would likely include equitable damages caused by the loss of privacy, for example, a breach of security resulting in an identity theft.

Information about Purdue's Computing Security Policies

Many of Purdue's existing policies already address some of the compliance issues in the GLBA Safeguards Rule.

- To view Purdue policies, visit <http://www.purdue.edu/policies/index.html> for information about computer security policies including:
 - » Authentication and Authorization
 - » Data Security and Access
 - » Privacy of Electronic Information
 - » Remote Access to IT Resources
 - » Proper Disposal of Electronic Media

Selected University Executive Memoranda

- No. B-50, Terms and Conditions of Employment of Faculty Members:
http://www.purdue.edu/oop/policies/pages/human_resources/b_50.html
- No. B-54, Requesting Social Security Numbers for Educational, Employment and Other Record Keeping Purposes:
http://www.purdue.edu/oop/policies/pages/human_resources/b_54.html
- No. B-55, Terms and Conditions of Employment of Administrative and Professional Staff:
http://www.purdue.edu/oop/policies/pages/human_resources/b_55.html
- No. C-2, Disclosure of University Records: Procedures for Use in Connection with the “Access to Public Records” Law, and in Response to Third-Party Subpoenas:
http://www.purdue.edu/oop/policies/pages/human_resources/c_2.html

Selected University Executive Memoranda (Continued)

- No. C-8, Policy for Security Standard Practice Procedures:
http://www.purdue.edu/oop/policies/pages/records/c_8.html
- C-10, Delegation of Administrative Authority and Responsibility to Officers Reporting to the President of the University:
http://www.purdue.edu/oop/policies/pages/governance/c_10.html
- No. C-34, Data Security and Access Policy Statement:
http://www.purdue.edu/oop/policies/pages/information_technology/c_34.html
- No. C-41, Assignment of Authority and Responsibility for the Retention and Disposal of University Records:
http://www.purdue.edu/oop/policies/pages/records/c_41.html
- No. C-51, University Policy Regarding the “Family Educational Rights and Privacy Act of 1974” (as amended):
http://www.purdue.edu/oop/policies/pages/records/c_51.html

For More Information at Purdue

- ITaP Security and Policy web page: <http://www.itap.purdue.edu/security/>
- Selected Purdue Information Technology Administrative Computing Guidelines or Policies:
<http://www.itap.purdue.edu/security/policies/guidelines.cfm>
- IT Selected Procedures
<http://www.itap.purdue.edu/security/policies/guidelines.cfm>
- IT Selected Guidelines
<http://www.itap.purdue.edu/security/policies/guidelines.cfm>
- IT Best Practices <http://www.itap.purdue.edu/security/policies/>
- Administrative Data Classifications & Information Owners web page:
<http://www.itap.purdue.edu/security/procedures/dataClassif.cfm>
- FERPA Guidelines at Purdue:
<http://www.purdue.edu/Registrar/Records/FERPA/index.htm>

Resources at these sites may alert you to new risks to information security and help those individuals whose information may have been compromised with their next steps.

- The Federal Trade Commission: <http://www.ftc.gov/>
- Additional guidance regarding GLBA is available at: <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

For More Information

In addition, the following organizations have information available to help you implement appropriate safeguards for your customer data:

- Computer Security Resource Center, The National Institute for Standards and Technology (NIST):
www.csrc.nist.gov
- Critical Infrastructure Assurance Office (CIAO):
www.ciao.gov
- System Administration, Networking and Security Institute (SANS) - www.sans.org
- The 20 Most Critical Internet Security Vulnerabilities -
www.sans.org/top20.htm

Who to Contact With Questions?

- Contact your manager for specific procedural questions in your area.
- Contact IT Security & Policy for Risk Assessments, educational materials, and help with computer security.
- To contact IT Security & Policy send e-mail to: itap-securityhelp@purdue.edu