FINANCIAL AID OFFICE

Objectives for Gramm Leach Bliley Act (GLBA) Training

- GLBA Overview
- Safeguards Rule
- GLBA Definitions

What is GLBA?

- The Gramm Leach Bliley Act (GLBA) is a comprehensive, federal law affecting 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 Federal Trade Commission (FTC) enforces compliance with GLBA.
- The FTC may bring an administrative enforcement action against any financial institution for non-compliance with the GLBA.
- The University of Alaska Fairbanks (UAF) significantly engages in student loan making and provides financial services to student customers. As such, UAF falls within the definition of "financial institution" under the GLBA and must comply with the law's requirements".
- "Financial Institution" means any institution the business of which is engaging in financial activities.
- The GLBA is composed of several parts, including:
  - the Privacy Rule (16 CFR 313) and
  - the Safeguards rule (16 CFR 314).
- The FTC has officially stated that any college or university that complies with the Federal Educational Rights and Privacy Act (FERPA) 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). UAF complies with FERPA guidance.
- The FTC has not made a similar exception for an institution of higher education with respect to the Safeguards Rule.
- The Safeguards Rule requires all financial institutions to develop an information security program designed to protect "customer information."
- UAF must comply with the Safeguards Rule.
- There are three types of safeguards that must be considered when a UAF department implements safeguards to protect the security, confidentiality, and integrity of customer information:
  - Administrative Safeguards
  - Technical Safeguards
  - Physical Safeguards

Administrative Safeguards include developing and publishing policies, standards, procedures and guidelines, and are generally within the direct control of a department, such as:

- **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.**
- **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 are also generally within a department's control and include:

- **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.**
- **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.**
- **Ensure the storage areas are protected against destructions 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 disposal of records containing customer personal information.**
    - **Shred or recycle customer information recorded on paper and store it in a secure area until the confidential 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 outdates customer information according to record retention policies.**

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.**

GLBA DEFINITIONS:

Customer information is any record containing non-public 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.

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 customer;**
- **Information otherwise obtained about a customer in connection with providing a financial product or service to the customer.**

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

- **Provided by a consumer to a financial institution;**
- **Resulting from any transaction with the consumer or any service performed for the consumer; or**
- **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 Non-Public Person 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**

Additional guidance regarding GLBA is available at:

http://www.ftc.gov/privacy/privacyinititatives/glbact.html