Information Security Awareness Training

Gramm-Leach-Bliley Act
(GLB Act)

The GLB Act training packet is part of the Information Security Awareness Training that must be completed by employees. Please visit the Human Resources website at http://www.uh.edu/admin/hr/training/UHSonline.htm to take the full training and to receive credit.

Information Security Awareness Training
Lesson Two – Gramm-Leach-Bliley Act (GLB Act)

Purpose of the Gramm-Leach-Bliley Act (GLB Act)

The Gramm-Leach-Bliley Act (GLB Act) is a federal law which mandates that financial institutions, including institutions of higher education, protect the security, confidentiality and integrity of customer information. 16 CFR § 314.1(a).

In this regard, the Federal Trade Commission has issued safeguarding rules that implement the GLB Act. These rules establish standards related to administrative, technical and physical safeguards.

The objectives of the GLB Act training are to educate employees on: (1) the requirements of the GLB Act; (2) how to identify customer information; and (3) how to safeguard customer information. The training information was derived, in part, from the GLB Act, the Code of Federal Regulations (16 CFR § 314) and the Federal Trade Commission.

What is the GLB Act?

- The GLB Act is a federal law, also known as the Financial Modernization Act of 1999.
- The GLB Act applies to financial institutions, including institutions of higher education such as the University of Houston System ("UHS") and component universities.
- The GLB Act directs appropriate agencies, such as the Federal Trade Commission ("FTC") to establish standards by which financial institutions must develop information security programs.
- The FTC has established safeguarding rules mandating that UHS and component universities "protect the security, confidentiality and integrity of customer information." 16 CFR § 314.1(a).

What are the objectives of the safeguarding rules?

- The objectives of the safeguarding rules are to:
- "Insure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer." 16 CFR § 314.3 (b)(1-3).

Who must abide by the GLB Act?

- UHS and component universities must abide by the GLB Act.

- All employees of UHS and component universities must abide by the GLB Act.

What does the GLB Act require?

- The GLB Act mandates that UHS and component universities safeguard financial information that is collected or maintained in connection with its financial institution activities.

- UHS and component universities must protect financial information in paper, electronic and other forms.

What is customer information?

Customer information is defined as "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 [UHS, its component universities or its] affiliates." 16 CFR § 314.2 (b).

Whose information must be safeguarded under the GLB Act?

UHS and component universities must safeguard all financial information in their possession, "regardless of whether such information pertains to individuals with whom [UHS or component universities have] a customer relationship, or pertains to the customers of other financial institutions that have provided such information to [another financial institution]." 16 CFR § 314.1 (b).

Examples include:

- applicants
- parents
- staff
- faculty
- donors

What type of information must be safeguarded under the GLB Act?

Generally, all customer information must be safeguarded. Examples include:

- credit card account numbers
- bank account numbers

- income histories
- credit histories

What are the potential risks of not safeguarding information?

Potential risks of not safeguarding information are:

- unauthorized access of financial information by third parties
- unauthorized transfer of data to third parties
- interception of data during transmission
- physical loss of data due to disaster or theft
- compromise of computer system security
- identity theft

How can employees avoid risks in daily operations?

Employee Training and Management

To avoid risks in operations concerning employee training and management, the FTC suggests, in part, that UHS and component universities:

- Check references before hiring new employees;

- Train employees to identify and properly collect and maintain customer information. Basic steps include:

    - using password protected screensavers;

    - changing passwords frequently (and not posting passwords at or near computers);

    - locking rooms and file cabinets where paper records are maintained;

    - encrypting customer information if it must be e-mailed;

    - recognizing fraudulent attempts to obtain customer information;

    - referring requests for customer information to designated employees;

- Limit access to customer information to only those employees who have a business reason for handling the information and to only such an extent that they need it to do their jobs.

Information Systems

To avoid risks in operations concerning information systems (including network and software design, as well as information processing, storage, transmission and disposal), the FTC suggests, in part, that UHS and component universities:

- Store records in a secure area. For example:
    - Store paper records in a locked room when such records are unattended;
    - Keep archived data secure by keeping them in a physically secure area or storing them off-line;
    - Ensure that storage areas are protected against physical hazards such as floods and fire;
    - Don’t store customer information on a computer with an internet connection. If you are connected the internet, encrypt and password protect the file.
- When collecting or transmitting customer information, provide for easy to understand and secure data transmission
    - Use a Secure Sockets Layer (SSL) or other secure connection for transmitting and collecting sensitive financial information (such as credit card information);
    - If an employee must use e-mail to transmit sensitive financial information, ensure that the content is encrypted and password protected;
    - Caution customers against transmitting sensitive financial information via electronic mail.
- Dispose of customer information appropriately and securely. For example:
    - Shred customer information and store it in a secure area until it is disposed of;
    - Erase all customer information from computers, diskettes, hard drives or other electronic media when disposing of these items;
    - Destroy all hardware that is to be disposed of.

Managing Information System Failures

To avoid risks in operations concerning information system failures (including the prevention, detection and response to attacks and intrusions), the FTC suggests, in part, that UHS and component universities:

- Maintain current controls by:
    - Installing anti-virus software that updates automatically;
    - Maintain current firewalls;
    - Regularly check with software vendors to install patches that correct software vulnerabilities;
    - Follow a written plan to address any breaches of physical, administrative or technical safeguards;
- Other suggestions for managing system failures are:
    - Back up all customer information regularly;
    - Combine the use of passwords and personal identifiers to authenticate the identity of customers who attempt to transact business electronically.
    - Notify the Information Security Program Coordinator so that he/she may notify customers if their nonpublic personal information is subject to unauthorized access, loss or damage.

For more information about the GLB Act safeguarding rules, please see the FTC's website at: http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm

Who do I contact if I do not know what to do?

- If you receive a request for a customer's financial information, refer the requestor to those university employees who have undergone information security training.
- If you suspect an attempt to fraudulently obtain a customer's financial information, immediately report the attempt to the Information Security Program Coordinator. Please refer to the UHS Resource page for contact information – System Wide Security Contacts. The Information Security Officer (ISO) will serve as the Information Security Program Coordinator. The Coordinator will interact with the Office of the General Counsel to implement the information security program. The Coordinator will also interact with appropriate University departments to facilitate safeguarding procedures.

GLB Quiz

1. The GLB Act mandates that financial institutions safeguard customers' financial information.
    - True
    - False

2. According to the GLB Act, UHS and component universities must protect customers' financial information that is maintained on floppy disks, cds and on computers.
    - True
    - False

3. According to the GLB Act, UHS and component universities must protect customers' financial information that is printed on paper.
    - True
    - False

4. An employee should place paper listings of customers' financial information in campus trash cans when he/she no longer uses the information contained in the paper listing.
    - True
    - False

5. An employee should place diskettes that contain customers' financial information in campus trash cans when he/she no longer uses the information contained on the diskette?
    - True
    - False

6. Customer information may be appropriately stored in an area which has flooded several times in the past, but which has been properly cleaned each time.
    - True
    - False

7. Employees may freely transmit financial information to customers and other employees via e-mail.
    - True
    - False

8. If customers' financial information is stolen, then an employee should keep this occurrence to him/herself so as not to cause disruption to UHS or component universities.
    - True
    - False

9. Employees should take affirmative steps to avoid risks in UHS and component university operations.
    - True
    - False

10. If an employee believes that customers' financial information has been or may be inappropriately released, then the employee should contact the Information Security Program Coordinator for his/her component university.
    - o True
    - o False

Answers

1. The correct answer is **true**. The GLB Act mandates that financial institutions take affirmative steps to safeguard customers' financial information. The GLB Act applies to UHS and component universities because these entities regularly engage in financial institution activities in their daily operations.

2. The correct answer is **true**. The GLB Act mandates that UHS and component universities safeguard customers' financial information no matter the form that it is in. So, items such as floppy disks and cds that contain customers' financial information should be locked in file cabinets and/or rooms when not in use. Computers should be password protected and otherwise secured against damage or loss. Floppy disks, cds and computer hardware that contain customers' financial information, should be deleted, stored in a secure area until destroyed, then disposed of.

3. The correct answer is **true**. The GLB Act mandates that UHS and component universities safeguard customers' financial information no matter the form that it is in. So, customers' financial information that is printed on paper should be locked in file cabinets and/or rooms when not in use. Paper copies should be shredded, then stored in a secure area until they are disposed of.

4. The correct answer is **false**. It is not appropriate to dispose of paper listings of customers' financial information by simply placing the hardcopies in campus trash cans. Paper listings of customers' financial information should be shredded, then stored in a secure area until they are disposed of.

5. The correct answer is **false**. It is not appropriate to dispose of diskettes, cds or computers that contain customers' financial information by simply placing these items in campus trash cans. Hardware that contains customers' financial information should be deleted, stored in a secure area until destroyed, then disposed of.

6. The correct answer is **false**. Customers' financial information must be safeguarded against damage and loss. Therefore, items containing customers' financial information (such as floppy disks, cds, computers, paper copies), should be stored in areas that are secured against hazards such as fire or flooding and in areas that are secured against theft.

7. The correct answer is **false**. Employees must take affirmative steps to ensure the confidentiality of customers' financial information. Therefore, if e-mail must be used, then some steps that employees should take to ensure the confidentiality of information are: to password protect the content of the e-mails and to combine the use of passwords and personal identifiers to authenticate the identity of customers who attempt to transact business electronically.

8. The correct answer is **false**. If customer information is stolen or if an employee suspects that such information is subject to unauthorized access, loss or damage, then the employee should immediately contact his/her component's Information Security Officer

who serves as the Information Security Program Coordinator. Compromised computer system security, identity theft and other risks could result if an employee does not report unauthorized access, loss or damage (or threats of access, loss or damage) to the Information Security Program Coordinator.

9. The correct answer is **true**. The safeguarding rules, in part, require UHS and component universities to avoid risks in operations by, maintaining current controls such as installing anti-virus software that updates automatically, maintaining firewalls and regularly checking with vendors to install patches that correct software vulnerabilities. Employees should also regularly back up customers' financial information contained in computer systems.

10. The correct answer is **true**. The Information Security Officer (ISO) for a component university serves as the Information Security Program Coordinator for that component university. If an employee suspects that customers' financial information has been or may be inappropriately released, then he/she should immediately contact the Information Security Program Coordinator.