Guarding Against Identity Theft

Gramm-Leach-Bliley Act (GLBA)

Red Flag Rules

&

Student Awareness

Presentation Begins at 11:00am Pacific Time

By Ruth Sharp, Bursar

Caltech

Overview

There were 16.7 million victims of identity fraud, a record high that followed a previous record the year before.[1] Due to rampant identity fraud, universities are becoming ever more governed by privacy and data security regulations such as FERPA, HIPA, GLBA, Red Flag Rules and EU General Data Protection, just to name a few.

Today's Webinar Agenda:

- GLBA Gramm-Leach-Bliley Act 1999

- 4 rules to protect consumer financial Information
  1. Financial Privacy Rule
  2. Safeguards Rule:
     Written information security program to protect privacy and integrity of customer data
  3. Red Flag Rule: implemented in 2010
     Written program to detect, prevent, mitigate identity theft pertaining to covered accounts
  4. Pretexting Protections

- Student Awareness

Today's Webinar Agenda

The GLBA, including both Safeguard and Red Flag Rules, require:

- Develop and maintain written procedures for a security plan and also for identifying red flags.
- Assess or detect risks
- Implement reasonable safeguards or rules
- Oversee service providers and educate staff
- Evaluate, monitor, and adjust these procedures
- And respond to both security breaches and red flags

DISCLAIMER:

- We are here to help!
- The information in this webinar is not intended to be legal advice and may not be used as legal advice.
- Effort has been made to ensure that we are providing updated information. This information should not be used in place of your schools general counsel or your own legal counsel.

Definitions

Identity Theft is a fraud committed or attempted using the personal identifying information of another person without authority.

A "**Red Flag**" is a pattern or practice, or specific activity that indicates the possible existence of identity theft.

Covered Accounts are continuing **relationships with third parties** that the school maintains primarily for personal, family or household purposes that involve or are designed to permit multiple payments or transactions. Covered accounts also **include any other account that the school offers or maintains for which there is a reasonably foreseeable risk to customers** or to the safety and soundness of the Institute or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

At the school, offices that engage in business processes that depend on identifying information for the purpose of creating accounts and associated activities such as mailing statements, receiving payments, viewing accounts online, promissory notes, notifications by e-mail or correspondence and telephone contacts **are subject to rules governing covered accounts**.

A **creditor** is a person or entity that bills after providing goods or services.

Overview:

The GLBA, (both Safeguard Rules and Red Flag Rules), require organizations to protect the privacy of consumer financial information.

Is your school a creditor?

Does your school regularly and in the course of business:

- Obtain or use consumer credit reports?
- Provide information to consumer reporting agencies?
- Advance funds which must be repaid in the future?

Caltech

Participatory Effort to Protect Customers

Develop a Campus Working Group

- Representatives from throughout the University
- President
- Provost
- Senior Officers, especially CIO
- Bursar or Student Financial Service Directors

Implement Procedures to Protect Customers

- Set policy and assign a manager for maintaining compliance
- Identify departments on campus who create or administer covered accounts
- Administer program to those departments:
  - Train department staff
  - Implement procedures to monitor red flags, and process identity theft claims
- Review and update P&P annually

GLBA Safeguard Rules

GLBA Risks and Mitigation - Safeguard Rules

- Compromise of computer system –

System may be compromised due to lack of effective protections.

Procedure to include firewalls, strong password policies, dual log in, update antivirus, and system patches. Educate about e-mail attachments and risk of using external storage devises.

- Unauthorized access, internal & external –

Internal: Procedure for "function based" permissions policy so users access may only what is required for their job function.

External: Procedure for locking computer when not physically at it, and also use timed screen saver. This helps to prevent key loggers, virus uploads, and physical removal of data.

GLBA Risks and Mitigation - Safeguard Rules

- Unauthorized Access –

Helpful to have practices of dual log in: key fob and password required.

Policy of smart passwords:

six characters long

contains both numeric and alpha characters

Abstain from use of family or pet names

- Unauthorized Access –

Policy to change password periodically

(ex. 30 to 90 days)

Strict policy enforced to never share passwords!

GLBA Risks and Mitigation - Safeguard Rules

- Interception of Data – Maintain a policy against unencrypted sensitive data. Use current industry recommended encryption, certificates and keys. Examples of secure delivery may include encrypted e-mail, delivery to a secure file location on a third party server, or use of a drop box.

- Corruption of Data & System: hijacked for ransom or due to disaster–
  - Policy to maintain a backup system.
  - Secure it:
  - Stand alone
  - Preferable offsite location for storage of the backed up data,

(offsite may include cloud)

GLBA Risks and Mitigation – Safeguard Rules

- Unauthorized transfer of data by 3rd parties–

Create a third party cyber policy.

Ensure that they perform PEN testing on their firewall.

Consider router with built in network security.

- Administrative Issues

Policy to perform background checks

And review references prior to hiring.

Require university confidentiality agreements to be signed by all staff

Policy to educate staff about identifying and reporting risks

GLBA
Safeguard Rules -Where to Report a Breach

- ***Immediately*** contact your supervisor. They will report to:
  - Chief Information Officer
  - Campus Security
  - Internal Audits
  - Controller
  - Information Technology Services

Red Flag Rules

Implement Procedures to Protect Customers

- Set policy and assign a manager for maintaining compliance
- Identify departments on campus who create or administer covered accounts
- Administer program to those departments:
  - Train department staff
  - Implement procedures to monitor red flags, and process identity theft claims
- Review and update P&P annually

GLBA Red Flag Rules - Implementation

- Follow your universities policies
- Paper documents, files, electronic media and electronic data backups should be stored in locked containers in locked rooms.
- Access to keys to these secured areas should be limited to employees with a legitimate need.
- Employees should not leave sensitive information unattended at their workstations.
- No visitors should be allowed unescorted access to the office.
- Personally identifiable information sent externally should be encrypted and password protected.
- Industry standards for electronic data security should be followed.
- Electronic equipment and storage devices should be appropriately erased or purged of data.

GLBA Red Flag Rules - Implementation

- Contracts with affected service providers should require that they comply with the Red Flag Rule and that they have appropriate policies and procedures in place to identify, detect, mitigate, and prevent identity theft.

- Exercise appropriate and effective oversight of service provider arrangements. Oversight may include a review of service providers' own Red Flag Rules programs and requirements that service providers notify your university of any security breaches.

- Departments that communicate with credit reporting agencies or Third Party agencies shall follow procedures for reporting of address or other information discrepancies between the school and the contracted third party when:
  - The school has an established continuing relationship with the consumer or borrower.
  - The school regularly and in the ordinary course of business, furnishes information to the schools third party or reporting agent.

- Information shall not be provided to outside agencies for which the school has no contract.

- Requests for information from non-contracted agents should be initiated by the student / loan recipient and requested in writing with a wet signature to the school - no fax requests, nor e-mail requests accepted!

What a Red Flag May Look Like

1. Account activity appears inconsistent with usual activity pattern

2. Notification by account holder of charges not made by him/her

3. Account access has been compromised

4. Account application that appears to have been altered

5. Identification documents that appear to have been altered and are not consistent with the appearance of the person claiming to be the existing customer

6. Information on the identification that differs from what the person presenting the identification provides

What a Red Flag May Look Like (Cont.)

7. A person's Social Security Number ("SSN") or student ID number is the same as another account holder's SSN or student ID number.

8. A person's identifying information is not consistent with information from Human Resources or the Registrar's Office.

10. Suspect validity of an address change request for an existing covered account.

8. Computer System Breaches:

- System is compromised
- Unauthorized account access by outside entities or staff

9. Claim by customer that they may be a victim or are a victim of identify theft

GLBA Pretext Protections

- Unauthorized requests for data -***pretext calling***

Meaning a false reason given to hide the truth. Being someone that they are not.

Request all account holders to authenticate.

Require written request.

Never provide information to anyone except the account holder.
(Third parties may receive the information directly from the account holder.)

Responses to a Red Flag

- Continue to monitor an account for evidence of identity theft.
- Investigate, Contact the customer.
- Change passwords, security codes, or other ways to access a covered account.
- Suspend or close the account.
- Reopening an account with a new account number.
- Or, not opening a new account.
- Request additional documentation to validate identity.
- Notify law enforcement.
- Determine that no response is warranted under the particular circumstances.

Responding to a Claim of Identity Theft
Possible Identity Theft or a Claim of Being a Victim of Identity Theft
Identity Theft Resolution Act: Effective January 1, 2017

Debt Collector shall:

- ❑ Start an investigation within 10 days of receiving the customers claim of identity theft.

- ❑ It is recommended to:
  - Ask for the dispute and required documents in writing.
  - Required documents include a police report, and a written statement and other information as listed in civil code 1788-18.(Ref. information request template)
  - Forward all correspondence that is received from an attorney to your legal department.
  - Conduct all follow up correspondence with in writing.

- ❑ Five correspondence templates, first created by the CAC, are available at the end of the presentation.
- ❑ They include Initial Contact, Document Request, Claim Denial, Accepted Claim and Creditor Notice.

Responding to a Claim of Identity Theft
Possible Identity Theft or a Claim of Being a Victim of Identity Theft
Identity Theft Resolution Act: Effective January 1, 2017

Debt Collector shall:

- ❑ Cease collection of the debt upon receipt of a police report being received.
- ❑ Notify the credit reporting agency of the dispute within 10 days.
- ❑ Send notice of your investigations determination to the debtor no later than 10 business days after concluding the review.
- ❑ Notify the credit reporting agency to delete information no later than 10 days after making the determination to stop collection activity.

Finally, the law prohibits selling the debt if the creditor has received notice that the debt collector has terminated debt collection activities due to a claim of identity theft.

Building Student Awareness

Student Information – The How and Why

How?

- Trash
- Online phishing
- Leaving your personal information around, including your mail box

Why?

- Credit card fraud
- Counterfeit documents like ID
- Medical services
- Cash your pay check

Student Check List
Secure Personal Information

- ❑ Lock your financial documents and records in a safe place.
- ❑ When at work, store your wallet or purse in a safe place. Also, keep your information secure from roommates or workers who come into your home.
- ❑ Limit what you carry. When you go out, take only the identification, credit, and/or debit card(s) that you may need. Leave your Social Security card locked at home.
- ❑ Guard your Social Security number and ask questions before deciding to share it.
- ❑ Ask if you may use a different kind of identification. Ask why they need it, how it will be used, and how they will protect it. You may also ask what happens if you don't provide the social security the number.
- ❑ Before you share any personal information ask why they need it and how they will safeguard it.

Student Check List
Secure Personal Information

- ❑ Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.

- ❑ Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.

- ❑ Take outgoing mail to post office collection boxes or to the post office. Check mailbox daily. If you won't be home for several days, request a "vacation hold" on your mail.

- ❑ Don't provide personal information on the phone or over the internet unless you are able to verify who is contacting you, or unless you initiated the contact. If a company that claims to have an account with you sends an email asking for personal information, don't click on links in the email. Instead, call the customer service number listed on your account statement. Ask whether the company really sent a request.

Student Check List
Secure Online Information

- ❑ Limit the amount of information that you post online about yourself. The information can be used to answer challenge questions on your accounts, and to get access to your banking or personal information. Limit access of your networking page to personal friends only. Do not post personally identifiable information such as your full name, social security number, address, phone number, or account numbers.

- ❑ Use a security software by installing an anti-virus, and an anti-spyware software.

- ❑ Keep security patches updated. Use password protection. Also, in order to avoid spyware or a computer virus, do not opening files, click on links, or download programs that are sent from an unfamiliar source.

- ❑ When logging in at the library, coffee shop, or any other public place to use a Wi-Fi connection, be aware that an “encrypted website” only protects information that you send. A “secure wireless network” protects all of the information on that network. A “lock” icon on the status bar of your internet browser means your information will be safe when it’s transmitted. Look for the lock before you send personal or financial information online.

Student Check List
Secure Online Information

- Avoid maintaining personal information on a laptop. If you need to store personal information on the laptop then protect it with a passcode. Refrain from using the "auto fill features" or selecting the "remember this passcode" option.

- Before you dispose of a computer use a wipe utility program to overwrite the hard drive.

- Before you dispose of a mobile device check your owner's manual, or the manufacturer's website for information on how to delete information permanently, after you have transferred information to the new device. Also, remove the SIM card.

- Use strong passwords with your laptop, credit, bank, and other accounts by using numbers letters and symbols. Also do not use names of people and places associated with your identity.

- **For full information to this article How to Keep Your Information Secure, access the link to this article at: http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure**

Report Identity Theft

What can you do if you are a victim?

Contact the credit reporting agency to put a “Fraud Alert” on your account

File a police report:

File a report with the Federal Trade Commission at:

https://www.ftc.gov/faq/consumer.../report-identity-theft

Close any inappropriate accounts.

Contact your creditors in writing to dispute charges that were not made by you.

Provide the information as found at:

- http://codes.findlaw.com/ca/civil-code/civ-sect-1788-18.html

Report Identity Theft

Credit Reporting Agencies:

- Equifax: 1-800-525-6285 www.equifax,.com
- Experian 1-888-397-3742 www.Experian.com
- TransUnion: 1-800-680-7289 www.transunion.com

Federal Trade Commission:

- *https://www.**ftc**.gov/faq/consumer.../**report-identity-theft***

References

- 2018 Identity Fraud: Fraud Enters a New Era of Complexity, Javelin Strategy & Research, 2017
- Achieving GLBA Compliance for Data Protection, https://a-lign.com posted july 24, 2018 by Andrew Mathieson
- NACUBO GLBA Template *https://www.nacubo.org/-/media/Nacubo/Documents/business.../model_04.ashx?la*
- FTC https://www.ftc.gov/consumer-protection/gramm-leach-bliley-act