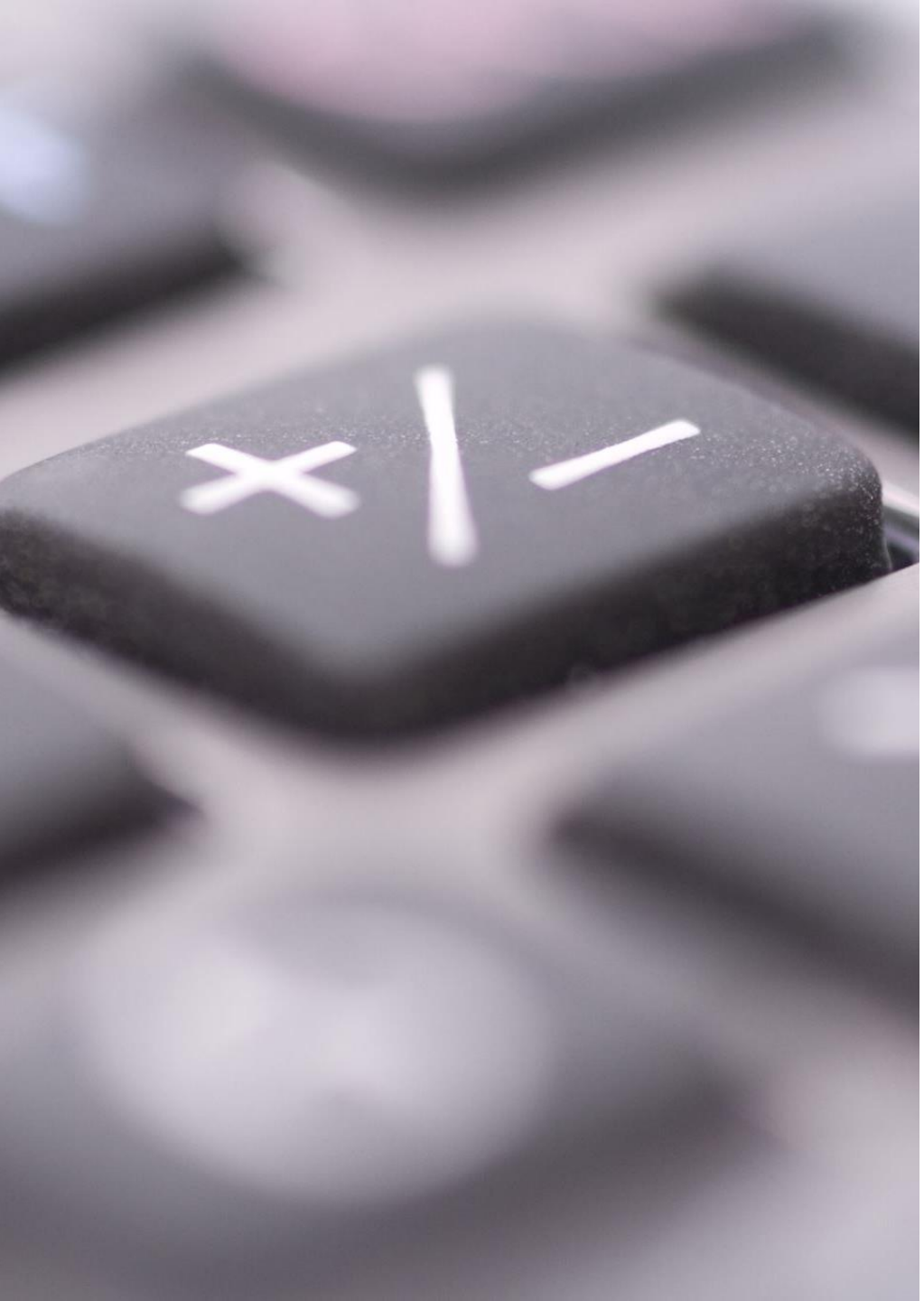

Cybersecurity and Identity Theft
Lisa Koretoff
Guilford TCC

Should I Care about Cybersecurity?

- Yes!
- You don’t have the power to implement most, if any, of the cybersecurity requirements, but someone on your campus does. This is like a lot of other federal requirements that don’t have anything to do with financial aid.
- This information is being reviewed during compliance audits.



The GTCC Experience

- Ransomware attack – Fall 2020
  - Immediately notified our System Office, the FBI, and the Department of Education.
  - Notified affected students and provided complimentary credit monitoring.
  - We had insurance!
- Two Dept of Ed Inspector General cases involving straw students.

FTC Red Flags Rule

Identity Theft Prevention Program

FTC Red Flags Rule

A good discussion on why colleges and universities are subject to the Red Flags rule can be found on the NACUBO website:

https://www.nacubo.org/Topics/Privacy-and-Data-Security/FTC-Red-Flags-Rule

Overview

FTC 16 CFR Part 681 - Identity Theft

16 CFR Part 681.2(d) Requires “establishment of an Identity Theft Prevention Program” and describes how to develop, implement, and administer one.

Four Basic Elements of an Identity Theft Program

Must include reasonable policies and procedures to identify the red flags of identity theft that may occur in your day-to-day operations.

Must be designed to detect the red flags you've identified.

Must spell out appropriate actions you'll take when you detect red flags.

Must detail how you'll keep it current to reflect new threats.

How to Comply Using the Four Elements - #1

Identify Relevant Red Flags

What are "red flags"? They're the potential patterns, practices, or specific activities indicating the possibility of identity theft.

- **Risk Factors -** When you are identifying key red flags, think about the types of accounts you offer or maintain; the ways you open covered accounts; how you provide access to those accounts; and what you know about identity theft in your business.
- **Sources of Red Flags -** Consider other sources of information, including the experience of other members of your industry. Technology and criminal techniques change constantly, so it's important to keep up-to-date on new threats.
- **Categories of Common Red Flags –** 26 red flags grouped in 5 categories to consider including in your program

How to Comply Using the Four Elements - #2

Detect Red Flags
Using identity verification and authentication methods can help you detect red flags. Consider whether your procedures should differ if an identity verification or authentication is taking place in person, by telephone, mail, or online.

- **New accounts -** for in-person verification, checking a current government-issued identification card, like a driver's license or passport. External sources of confirmation may include the Residency Determination Service.

- **Existing accounts -** Your program may include reasonable procedures to confirm the identity of the person you're dealing with, to monitor transactions, and to verify the validity of change-of-address requests. For online authentication, consider the Federal Financial Institutions Examination Council's guidance on authentication as a starting point. It explores the application of multi-factor authentication techniques in high-risk environments, including using passwords, PINs, smart cards, tokens, and biometric identification. Certain types of personal information — like a Social Security number, date of birth, mother's maiden name, or mailing address — are not reliable authenticators because they're so easily accessible.

- You and your third-parties may already be using programs to monitor transactions (like Positive Pay), identify behaviors that indicate the possibility of fraud and identity theft, or validate changes of address. If so, incorporate these tools into your program.

How to Comply Using the Four Elements - #3

Prevent And Mitigate Identity Theft

When you spot a red flag, be prepared to respond appropriately. Your response will depend on the degree of risk posed. It may need to accommodate other legal obligations, like laws about providing and terminating service.

- The Guidelines in the Red Flags Rule offer examples of some appropriate responses, including:
  - monitoring a covered account for evidence of identity theft
  - contacting the customer
  - changing passwords, security codes, or other ways to access a covered account
  - closing an existing account
  - reopening an account with a new account number
  - not opening a new account
  - notifying law enforcement
  - determining that no response is warranted under the particular circumstances.
- The facts of a particular case may warrant using one of these options, several of them, or another response altogether. Consider whether any aggravating factors raise the risk of identity theft. For example, a recent breach that resulted in unauthorized access to a customer's account records would call for a stepped-up response because the risk of identity theft rises, too.

How to Comply Using the Four Elements - #4

Update The Program

- The Rule recognizes that new red flags emerge as technology changes or identity thieves change their tactics and requires periodic updates to your program. Factor in your own experience with identity theft; changes in how identity thieves operate; new methods to detect, prevent, and mitigate identity theft; changes in the accounts you offer; and changes in your business, like mergers, acquisitions, alliances, joint ventures, and arrangements with service providers.

Administering Your Program

Your Board of Trustees — or an appropriate committee of the Board — must approve your initial plan. If you don't have a board, someone in senior management must approve it. The Board may oversee, develop, implement, and administer the program — or it may designate a senior employee to do the job. Responsibilities include assigning specific responsibility for the program's implementation, reviewing staff reports about compliance with the Rule, and approving important changes to your program.

Administering Your Program

The Rule requires that you train relevant staff only as “necessary.” Staff who have taken fraud prevention training may not need to be re-trained. Remember that employees at many levels of your organization can play a key role in identity theft deterrence and detection.

In administering your program, monitor the activities of your service providers. If they’re conducting activities covered by the Rule — for example, providing customer service or collecting debts — they must apply the same standards you would if you were performing the tasks yourself. One way to make sure your service providers are taking reasonable steps is to add a provision to your contracts that they have procedures in place to detect red flags and either report them to you or respond appropriately to prevent or mitigate the crime. Other ways to monitor your service providers include giving them a copy of your program, reviewing the red flag policies, or requiring periodic reports about red flags they have detected and their response.

It’s likely that service providers offer the same services to a number of client companies. As a result, the Guidelines are flexible about service providers using their own programs as long as they meet the requirements of the Rule.

Administering Your Program

The person responsible for your program should report at least annually to your Board of Trustees or a designated senior manager. The report should evaluate how effective your program has been in addressing the risk of identity theft; how you're monitoring the practices of your service providers; significant incidents of identity theft and your response; and recommendations for major changes to the program.

The 26 Red Flags

Adopt the ones that make sense for your college!

The 26 Red Flags

Institutions can incorporate Red Flags from the sources recommended in section II.b. of the Guidelines in appendix A of this part:

Sources of Red Flags. Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

- Incidents of identity theft that the financial institution or creditor has experienced;
- Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
- Applicable supervisory guidance.

In addition, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

The 26 Red Flags

Alerts, Notifications or Warnings from a Consumer Reporting Agency	1. A fraud or active duty alert is included with a consumer report.	
	2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.	
	3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 641.1(b) of this part.	
	4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:	a. A recent and significant increase in the volume of inquiries; b. An unusual number of recently established credit relationships; c. A material change in the use of credit, especially with respect to recently established credit relationships; or d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

The 26 Red Flags

Suspicious Documents	5. Documents provided for identification appear to have been altered or forged.
	6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
	7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
	8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
	9. An application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

The 26 Red Flags

Suspicious Personal Identifying Information	10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:	a. The address does not match any address in the consumer report; or
		b. The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
	11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.	
	12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:	a. The address on an application is the same as the address provided on a fraudulent application; or
		b. The phone number on an application is the same as the number provided on a fraudulent application.
	13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:	a. The address on an application is fictitious, a mail drop, or a prison; or
		b. The phone number is invalid or is associated with a pager or answering service.

The 26 Red Flags

Suspicious Personal Identifying Information (con't)	14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
	15. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or by other customers.
	16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
	17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
	18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

The 26 Red Flags

Unusual Use of, or Suspicious Activity Related to the Covered Account	19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.	
	20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:	a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
	21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:	Nonpayment when there is no history of late or missed payments; A material increase in the use of available credit; A material change in purchasing or spending patterns; A material change in electronic fund transfer patterns in connection with a deposit account; or A material change in telephone call patterns in connection with a cellular phone account.

The 26 Red Flags

Unusual Use of, or Suspicious Activity Related to the Covered Account (con’t)	22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
	23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
	24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
	25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

The 26 Red Flags

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Gramm-Leach-Bliley Act Safeguards Rule

Gramm-Leach-Bliley Act (GLBA) and the Safeguards Rule

Definition of "Customer" for Purposes of GLBA Compliance

“The regulations at 16 C.F.R. Part 314 use the terms “customer” and “customer information.” For the purpose of an institution’s or servicer’s compliance with GLBA, customer information is information obtained as a result of providing a financial service to a student (past or present). Institutions or servicers provide a financial service when they, among other things, administer or aid in the administration of the Title IV programs; make institutional loans, including income share agreements; or certify or service a private education loan on behalf of a student.”

(GENERAL-23-09) Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements, dated February 9, 2023, effective date June 9, 2023

GLBA and the Safeguards Rule

Background

"Postsecondary institutions and third-party servicers must protect student financial aid information provided to them by the Department or otherwise obtained in support of the administration of the Federal student financial aid programs (Title IV programs) authorized under Title IV of the Higher Education Act of 1965, as amended (HEA). Each institution that participates in the Title IV programs has agreed in its Program Participation Agreement (PPA) to comply with the GLBA Safeguards Rule under 16 C.F.R. Part 314. Institutions and servicers also sign the Student Aid Internet Gateway (SAIG) Enrollment Agreement, which states that they will ensure that all Federal Student Aid applicant information is protected from access by, or disclosure to, unauthorized personnel, and that they are aware of and will comply with all of the requirements to protect and secure data obtained from the Department's systems for the purposes of administering the Title IV programs."

(GENERAL-23-09) Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements, dated February 9, 2023, effective date June 9, 2023

Where to Start?

“In April of 2022, the FTC issued a new publication entitled FTC Safeguards Rule: What Your Business Needs to Know, which is meant to act as a “compliance guide” to ensure that entities covered by the Safeguards Rule maintain safeguards to protect the security of customer information. The publication provides valuable information such as describing what a reasonable security program should look like and goes over each of the nine required elements in greater detail.”

(GENERAL-23-09) Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements, dated February 9, 2023, effective date June 9, 2023

9 Elements of an Information Security Program

- Designate a qualified individual
- Conduct a risk assessment
- Design and implement safeguards based on risk assessment results – 8 Steps
- Test and monitor
- Train your staff
- Oversight of information system service providers
- Keep your program current
- **Create an incident response plan*
- **Report on information security program*

**only for institutions with 5000 or more "customers".*

8 Steps to Design/Implement Safeguards

1. **Implement and periodically review access controls.** Determine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it.

2. **Know what you have and where you have it.** Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted. Keep an accurate list of all systems, devices, platforms, and personnel. Design your safeguards to respond with resilience.

3. **Encrypt customer information on your system and when it's in transit.** If it's not feasible to use encryption, secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.

4. **Assess your apps.** If your company develops its own apps to store, access, or transmit customer information – or if you use third-party apps for those purposes – implement procedures for evaluating their security.

5. **Implement multi-factor authentication for anyone accessing customer information on your system.** For multi-factor authentication, the Rule requires at least two of these authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token), and an inherence factor (for example, biometric characteristics).

6. **Dispose of customer information securely.** Securely dispose of customer information no later than two years after your most recent use of it to serve the customer, unless you have a legal reason to keep it longer (state retention rules?)

7. **Anticipate and evaluate changes to your information system or network.** Changes to an information system or network can undermine existing security measures. For example, if your company adds a new server, has that created a new security risk? Because your systems and networks change to accommodate new business processes, your safeguards can't be static. The Safeguards Rule requires financial institutions to build change management into their information security program.

8. **Maintain a log of authorized users' activity and keep an eye out for unauthorized access.** Implement procedures and controls to monitor when authorized users are accessing customer information on your system and to detect unauthorized access.

Who’s gonna make me?

- Colleges will be evaluated via their compliance audit!
- Colleges without data breaches or compromised systems would have to submit a Corrective Action Plan (CAP) to remedy.
- Colleges with repeated noncompliance could lose their Title IV programs.

What's Next?

NIST 800-171 Rev. 2 Standards

- The Department is promising to issue guidance on NIST 800-171 compliance in a future Electronic Announcement.
- Colleges must protect controlled unclassified information (CUI). What is CUI? It is information owned or created by the government which is sensitive but not classified. Sound familiar?
- Encourages colleges to begin incorporating these information security controls under NIST 800-171 "as soon as possible". There are 110 requirements that cover access control, systems configuration, and authentication procedures.

(GENERAL-23-09) Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements, dated February 9, 2023, effective date June 9, 2023

Resources

- Appendix A to Part 681 – Interagency Guidelines to Identity Theft Detection, Prevention, and Mitigation https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681/appendix-Appendix%20A%20to%20Part%20681
- Data Security: K-12 and Higher Education https://studentprivacy.ed.gov/Security
- Federal Financial Institutions Examination Council Authentication and Access to Financial Institution Services and Systems https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf
- FSA Cybersecurity Announcements and Guidance https://fsapartners.ed.gov/knowledge-center/topics/fsa-cybersecurity-announcements-and-guidance

Resources

- FTC Safeguards Rule: What your Business Needs to Know https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
- Quarterly Cybersecurity Newsletter from FSA
  To sign up and receive FSA's new cybersecurity newsletter, please email FSASchoolCyberSafety@ed.gov with the subject line: "Send me the FSA Cybersecurity Newsletter for IHEs." Those who sign up will be added to the list to receive this quarterly newsletter.
- (GENERAL-23-10) New Cybersecurity Resources for Institutes of Higher Education Available https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-16/new-cybersecurity-resources-institutes-higher-education-available

Resources

- (GENERAL-23-09) Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements

NCASFAA would like to thank our Professional Affiliates!

College Foundation of North Carolina

DISCOVER Student Loans

Citizens One Student Loans™

SallieMae

PNC