The webcast will start at 1:00 p.m. Eastern

- Visit capincrouse.com/glba-updates-1 to access these materials from today's webcast:
  - Handouts
  - Recording
- To receive CPE credit, you must respond to the polling questions, which are not available on mobile devices. Please log in on a computer if you would like to receive CPE credit.
- CPE certificates will be emailed to you within the next few weeks.

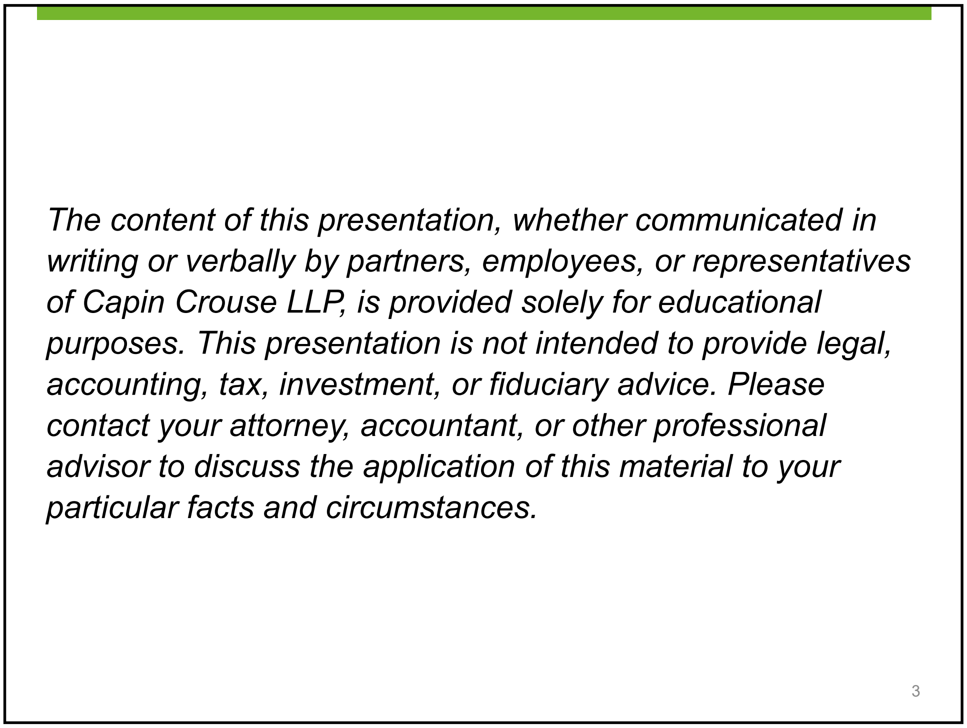
CAPINCROUSE LLP

Important GLBA Updates

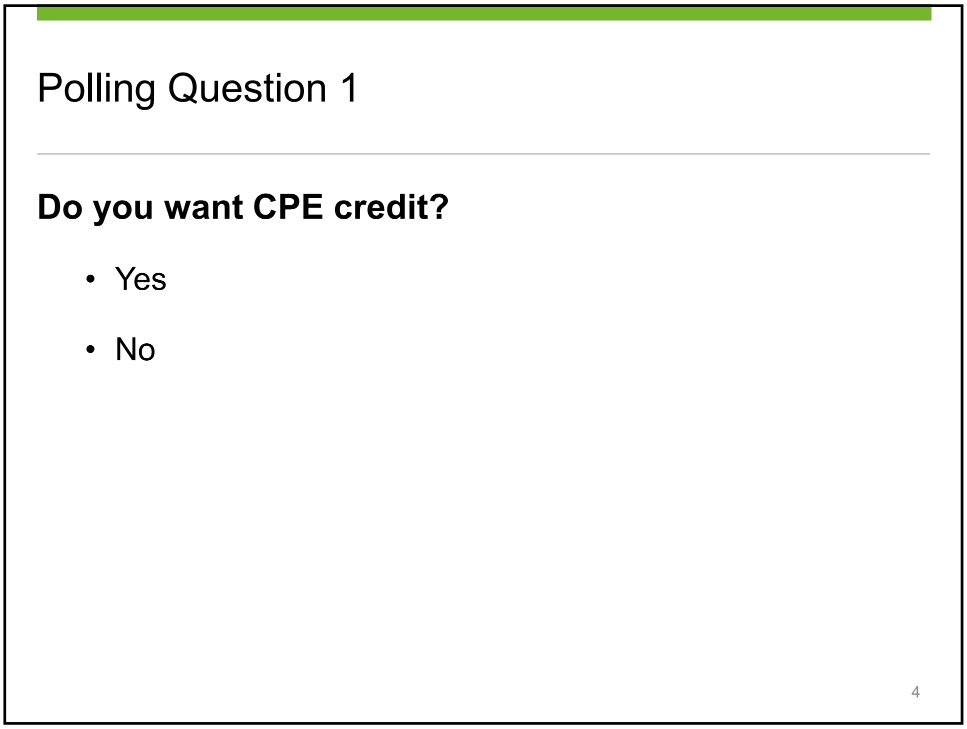
Part 1

Allison Ward, Partner, CapinTech
Patricia Willhite, Senior Manager, CapinCrouse
04.19.23

CAPINCROUSE LLP



The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, tax, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.



Polling Question 1

Do you want CPE credit?

- Yes
- No

Objectives for Today

- What is GLBA and why is it important?
- Does compliance equal security?
- What has changed over the years?
- What do I need to do to implement?

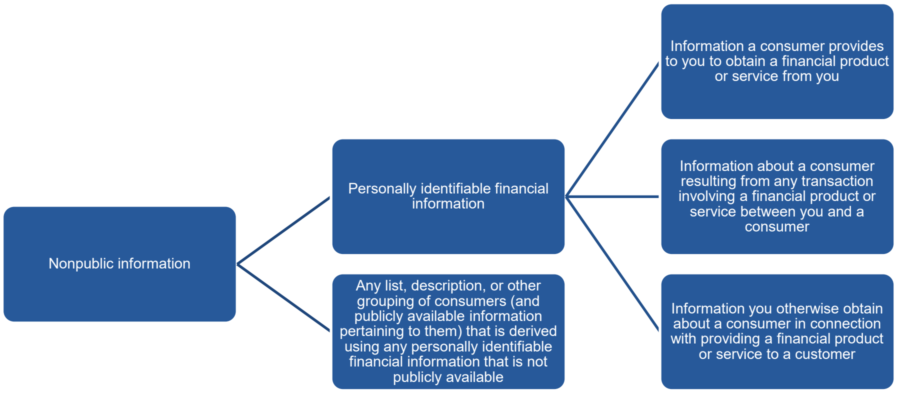
Who, What, When, and Why?

CAPINCROUSE LLP

What is the Safeguards Rule?

Who are my customers?

What is covered information?



Nonpublic information

Personally identifiable financial information

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

Information a consumer provides to you to obtain a financial product or service from you

Information about a consumer resulting from any transaction involving a financial product or service between you and a consumer

Information you otherwise obtain about a consumer in connection with providing a financial product or service to a customer

Examples, please?

- Personal info gathered from financial aid application
- Payment history, credit history, balance information
- Confirmation that the individual is or was your student
- Information collected through an Internet “cookie”
- Information from a consumer report

Polling Question 2

Are you compliant with GLBA?

- We’re good to go! Fully compliant.
- Partially compliant and working on it.
- We have a lot of work to do.

Why should we comply?

- We don’t want to lose federal funding.
- We care about our students.
- We want to carry out our mission for years to come.

Noncompliance resulting in a breach of covered information could impact all the above.

But we are REALLY small…

- Exceptions exist if you maintain data on fewer than 5,000 customers
  - 314.4(b)(1) – written risk assessment
  - 314.4(d)(2) – continuous monitoring
  - 314.4(h) – written incident response plan
  - 314.4(i) – annual report to the Board
- Should still be considered

13

All of this sounds good, so why is it so hard?

14

Then came the update…

- Provided more clarity on what is required
- Elaborated on expectations for safeguards
- Provided exceptions for compliance
- Extended effective date to June 9, 2023

15

Key Components of the Safeguard Rule

CAPINCROUSE LLP

§ 314.4(a) – Designate Your Qualified Individual

- Oversees, implements, and enforces your information security program (program)
- Considerations:
  - In-house vs. outsourcing
  - Within IT vs. independent of IT

17

Polling Question 3

Who is your Qualified Individual?

- Our CFO
- Our Financial Aid Coordinator
- Our IT Manager
- Separate Information Security Officer
- We have a committee

18

§ 314.4(b) – Conduct Your Risk Assessment

- Identify reasonably foreseeable risks to the security, confidentiality, and integrity of customer information
- Write it down, or it does not count!
- Perform periodically

What can a risk assessment look like?

Risk Area	Impact	Controls	Residual Risk	Potential Points of Exposure
Management has an inadequate understanding of information security threats and controls. **§ 314.4(i)**	• Management does not prioritize funding, staffing, or resources needed to ensure security. • There is inadequate support for information security initiatives.	• The Board receives an annual status report on the information security program. • The Chief Information Security Officer ("Qualified Individual") provides an update at each Board meeting and staff meeting. • An IT Committee meets monthly and is comprised of departmental leaders to facilitate buy-in for security initiatives. • Information security training is conducted annually for all employees.	Low	• Training attendance is not enforced, and departmental leaders and Management may not complete it.
Patch and vulnerability management procedures are weak.	• Increased risk of exploitation by hackers and malware. • Exposure of sensitive data. • Financial impact due to penalties, fines, and other expenses related to breach of sensitive data.	• External vulnerability scans are performed two times per year. • Anti-virus protection is installed on all servers, desktops, and laptops, and protections are monitored by IT staff weekly via a centralized console. • Automatic updates are configured on endpoints and end users are encouraged to apply security updates promptly.	High	• Internal vulnerability scans have not been performed in over two years. • Patch management protections are not enforced through a centralized management tool.

What are the biggest threats to your institution?

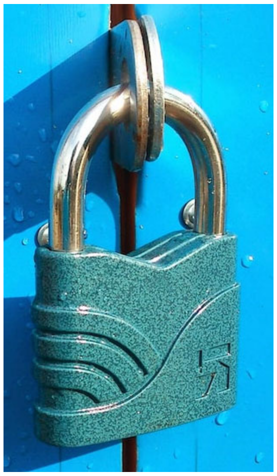
Windows Security

Windows Security

Threats found
Microsoft Defender Antivirus found threats. Get details.

But what do you do with the risk assessment?

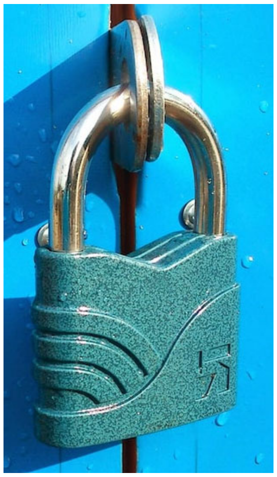
§ 314.4(c) – Implement Your Safeguards



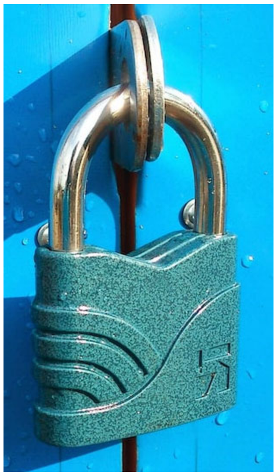
- Implement and periodically review technical and physical access controls
  - Limit access to approved users (authentication)
  - Limit access to support business need or job function (authorization)

§ 314.4(c) – Implement Your Safeguards

- Inventories of data, personnel, devices, systems, and facilities
  - You can’t manage what you can’t measure.
  - Do you know where your covered data is, who can access it, and how?



§ 314.4(c) – Logical and Physical Access Control

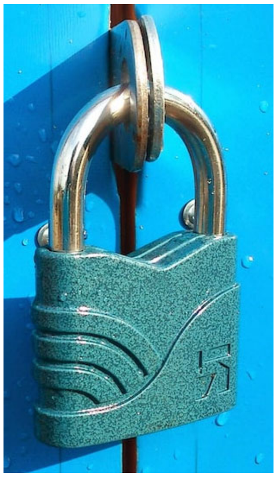


- Encryption of customer information
  - Start with your inventory
  - In transit vs. at rest
  - What to do with exceptions

25

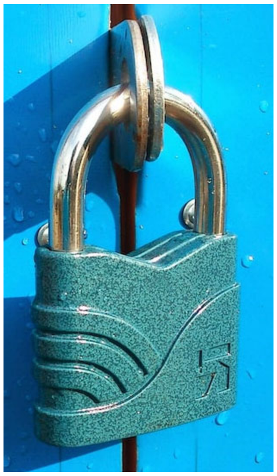
§ 314.4(c) – Implement Your Safeguards

- Application development procedures
  - Initial development
  - Ongoing evaluation and testing



26

§ 314.4(c) – Implement Your Safeguards



- Multi-factor authentication (MFA)
  - Any individual accessing any information system
  - What to do with exceptions

27

Polling Question 4

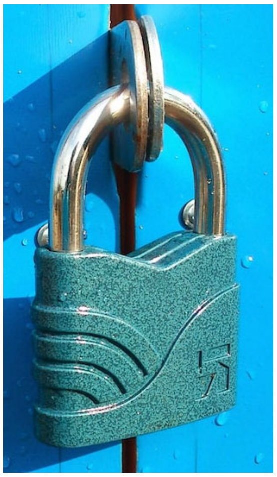
Are you using multi-factor authentication on your systems?

- All systems with personality identifiable information
- All of our vendor-hosted systems
- Some systems, but we could do more
- We need to implement MFA

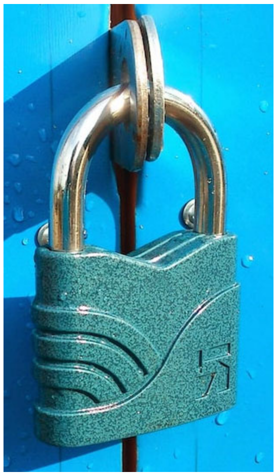
28

§ 314.4(c) – Implement Your Safeguards

- Data retention requirements and secure disposal procedures
  - What do you need to dispose of?
  - When do you need to dispose of it?
  - Why is data retention a good general security practice?



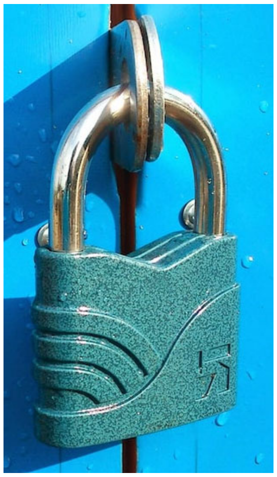
§ 314.4(c) – Implement Your Safeguards



- Change management
  - What constitutes a change?
  - What procedures should be defined?
  - Goal: implement changes to systems in a secure and controlled manner to limit the impact to customer data

§ 314.4(c) – Implement Your Safeguards

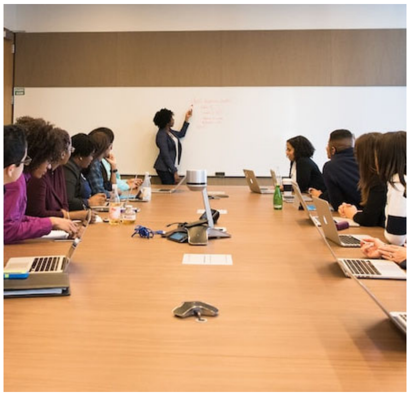
- Policies, procedures, and controls to monitor and log activity
  - Do you have visibility into your systems?
  - Do you log critical activity?
  - Do you monitor activity?



§ 314.4(g) – Update Your Program

- As a result of testing, monitoring, or ongoing risk assessments
- When there are material changes to your operations or environment
- Whenever something happens that materially impacts your program

§ 314.4(i) – Regularly Report to Your Board



- Overall status
- Risk assessment, risk management, and control decisions
- Service providers
- Results of testing
- Security events/violations
- Suggestions for changes

Don’t discount the power of the board report.

- Do not make this a “checklist” item.
- This is facetime with key decision makers.
- Get the buy-in and support for initiatives.
- Help them understand that GLBA is *their* responsibility.

Join Us for Part 2 on September 13

Join us for **Important GLBA Updates, Part 2** on September 13 at 1 p.m. EDT!

Scan the QR code or visit capincrouse.com/events to register for this free webcast.

Thanks!

Allison Ward, Partner
CapinTech, a CapinCrouse Company

✉ award@capincrouse.com
📱 505.50.CAPIN ext. 2008

Patricia Willhite, Senior Manager
CapinCrouse

✉ pwillhite@capincrouse.com
📱 505.50.CAPIN ext. 2030