Campus Cybersecurity and Data Privacy – The Path Forward

ABHES 18th Annual National Conference on Allied Health Education

New Orleans, Louisiana

March 10, 2022

MAYNARD COOPER GALE

PRESENTERS

- **Brandon Sherman** - Maynard Cooper & Gale
- **Starr Drum** - Maynard Cooper & Gale
- **Roger Swartzwelder** - Maynard Cooper & Gale

LEGAL DISCLAIMER

- *The purpose of this presentation is to provide news and information on legal and regulatory issues, and all content provided is for informational purposes only. It should not be considered legal advice.*
- *The transmission of information from this presentation does not establish an attorney-client relationship with the participant or reader. The participant or reader should not act on the information contained in this presentation or any accompanying materials without first consulting retained legal counsel.*
- *If you desire legal advice for a particular situation, you should consult an attorney.*

HIGHER EDUCATION PRACTICE

- The Higher Education Practice Group is deeply experienced in all manner of regulatory issues that are important to institutions, investors, third-party servicers, and accrediting agencies.

Title IV	**Accreditation**	**State Licensure**
Cybersecurity	**False Claims Act**	**Title IX**
Transactions	**Government Relations**	**Government Investigations**

CYBERSECURITY & PRIVACY PRACTICE

BTI CONSULTING GROUP
LITIGATION LEADER 2022

- Recognized by corporate counsel as "best of the best" in *BTI Litigation Outlook 2022*

BTI CYBERSAVVY 2020
Excellence in Cybersecurity & Data Privacy

Privacy & Cybersecurity Compliance

Breach Response

Privacy Litigation & Regulatory Investigations

Transaction & Risk Advisory Services

MAYNARD COOPER GALE

RECENT CYBER TRENDS

- **Ransomware** attacks and **extortion** attacks have been rampant.
- **Business email compromise** schemes continue to plague organizations of all industries.
- Data breach **costs** continue to grow. Average cost of a data breach in 2020 in the education sector was **$3.9M**.

INSTITUTIONS ARE TARGETED BY CYBERCRIMINALS

- They collect and store a high volume of **sensitive data** (financial information & PII).
- The **operational impact** of a cyber attack could be crippling … and criminals know this.
- Increased vulnerabilities due to **COVID-19**.

CYBERSECURITY/DATA PRIVACY COMPLIANCE

- Gramm-Leach-Bliley Act (GLBA)
- Student Aid Internet Gateway (SAIG)
- NARA CUI Rule/NIST SP 800-171
- HEA data use sharing limitations (20 U.S.C. 1090)
- Family Educational Rights and Privacy Act (FERPA) (and state-specific student privacy laws)
- California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA)
- Forthcoming comprehensive privacy laws in Virginia, Colorado, and Utah
- FTC Act

APPLICABLE DEPARTMENT REGULATIONS

Administrative Capability (34 C.F.R. § 668.14)

- To begin and continue participation in Title IV programs, an institution must maintain appropriate institutional capability for the sound administration of Title IV programs.
  - The maintenance of adequate checks and balances in IHEs **systems of internal control**.

PROGRAM PARTICIPATION AGREEMENT

- Institutions of higher education agree to comply with the **GLBA**, Safeguards Rule.
- "Institutions are strongly **encouraged to inform** its students and the Department of any breach."
- "The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability."

GLBA AUDIT

- Added to the Compliance Supplement and **OIG Audit Guide** in 2019.
- Audit Procedures
  - Verify that the institution has designated an individual to coordinate the **information security program.**
  - Verify that the institution has performed a **risk assessment** that addresses the three required areas
    - Employee training
    - Information systems
    - Detecting, preventing, and responding to attacks
  - Verify that the institution has documented a **safeguard** for each risk identified above.

SAIG

- Federal Student Aid Application Systems (e.g., COD & NSLDS)
- Must ensure that Title IV data is protected from access by or disclosure to unauthorized personnel
- Must **immediately notify** the Department of a breach
- GLBA compliance requirement
- Institutions' **point of contact** information

BREACH NOTIFICATION

- Includes a suspected breach
- How to report a breach:
  - cpssaig@ed.gov
  - Include date of the incident, impact of breach, remediation status
- Keep in mind overlapping state data breach notification laws.

GLBA OVERVIEW

Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 (Pub. L. No. 106-102)

GLBA requires financial institutions to provide customers with information about the institutions' privacy practices and their opt-out rights and to implement security safeguards.

Subtitle A of Title V of the GLBA requires the FTC to issue regulations requiring financial institutions to develop standards relating to physical safeguards for certain information.

GLBA OVERVIEW

- GLBA applies to the handling of "customer information" by **financial institutions**.
- GLBA applies to entities engaged in "financial activities."
  - **Postsecondary institutions** are considered financial institutions by the FTC.
- GLBA is **enforced by the FTC** for non-banking financial institutions.

RULEMAKING

- The FTC is required to periodically review all of its rules and guidance.
- On April 4, 2019, the FTC issued a **Notice of Proposed Rulemaking** setting forth proposed amendments to the Safeguards Rule. https://www.govinfo.gov/content/pkg/FR-2019-04-04/pdf/2019-04981.pdf
- The FTC received 28 public comments, including some by the American Council on Education.

FINAL RULE OVERVIEW

- On **December 9, 2021**, the FTC issued a Final Rule to amend the GLBA, Safeguards Rule. (86 FR 70272) https://www.govinfo.gov/content/pkg/FR-2021-12-09/pdf/2021-25736.pdf
- The Final Rule is intended to "strengthen[] the data security safeguards that financial institutions are required to put in place to protect their customers' financial information."
- The FTC's Commission voted 3-2 to adopt the final revisions to the Rule.

FINAL RULE OVERVIEW

- The Final Rule modifies GLBA in several key ways:
  - More detailed requirements for the development and establishment of an information security program.
  - Adds requirements designed to improve accountability of financial institutions' information security programs.
  - Includes several definitions and related examples, including of "financial institution."

KEY CHANGES

- The Final Rule requires that financial institutions prepare a **written risk assessment**. This assessment must include or address each of the following items:
  - Criteria for **evaluating identified risks** faced by the financial institution;
  - Criteria for the **assessment** of the confidentiality, integrity, and availability of the financial institution's information systems and customer protection; and
  - How **identified risks** will be mitigated or accepted.

KEY CHANGES

- **Incident response plan**:
  - Requires financial institutions to develop and implement an incident response plan.
  - Incident response plan must address:
    - Goals of the plan
    - Processes for responding to a security event
    - Roles and responsibilities
    - Information sharing
    - Remediation of any identified weakness
    - Documenting and reporting security events
    - Evaluating and revising response plan following security event

KEY CHANGES

- The Final Rule requires financial institutions to design and implement **safeguards to control risks**, including by:
  - Access controls
  - Encryption
  - Change management
  - Multi-factor authentication
  - Disposal of customer information
  - Monitoring access

KEY CHANGES

- Requires financial institutions to "**periodically assess**" their service providers on an ongoing basis.
  - Continues the requirements to based on the risk they present and the continued adequacy of their safeguards.

KEY CHANGES

Financial institutions must designate a **"Qualified Individual"** responsible for overseeing and implementing its information security program and enforcing its information security program.

KEY CHANGES

- The qualified individual must submit an **information security report** in writing and at least annually to the institution's board of directors or equivalent governing body.
- The report shall include the following information:
  - The overall status of the information security program and the financial institution's compliance with the Rule; and
  - Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations, and recommendations for changes in the information security program.

KEY CHANGES

- **Training requirements** include:
  - Providing **all personnel** with security awareness training; and
  - **Verifying** that key **information security personnel** take steps to maintain current knowledge of changing information security threats and countermeasures.

KEY CHANGES

- **Small Businesses**
  - The Final Rule exempts financial institutions that collect information about fewer than **5,000 consumers** from the following:
    - Written risk assessment
    - Incident response plan
    - Annual reporting requirements

EFFECTIVE DATE

- This Final Rule became effective on **January 10, 2022**.
- However, certain provisions will become effective on **December 9, 2022**.
  - Provisions include:
    - Appointment of a qualified Individual
    - Written risk assessments
    - Written incident response plan

SUPPLEMENTAL NOTICE

- **Notification requirement**
  - The FTC is issuing a Supplemental Notice of Proposed Rulemaking that proposes adding a requirement that financial institutions notify the FTC of detected security events under certain circumstances.

GLBA NON-COMPLIANCE

- **Enforcement options**
  - U.S. Department of Education
  - FTC

NIST SP 800-171 BACKGROUND

- Executive Order 13556
- NARA CUI rule (32 C.F.R. Part 2000)
  - Applies to Controlled Unclassified Information (CUI)
  - Agreement requirement

National Institute of Standards and Technology
U.S. Department of Commerce

SECURITY REQUIREMENT FAMILIES

Access Controls	Configuration Management
Awareness and Training	Identification and Authentication
Audit and Accountability	Incident Response
Maintenance	Media Protection
Personnel Security	Physical Protection
Risk Assessment	Security Assessment
System and Communications Protection	System and Information Integrity

PRIVACY V. SECURITY

4 Ps OF PRIVACY

- People
  - Types (individually and based on relationship with privacy notice provider)
  - Categories of information
- Places
- Platforms
- Purpose

COMPLIANCE PROGRAM

- What do we collect?
- Do we need it?
- What laws apply?
- Develop notice and consent documentation and process.
- Ensure protection/security of data.
- Develop and implement retention/deletion process.
- Train.
- Audit uses.

INSTITUTIONAL LEADERSHIP

- Presidents and Chief Information Officers of institutions should have, at a minimum:
  - Evaluated and documented their current posture against the requirements of GLBA and other applicable state and federal privacy and cybersecurity laws; and
  - Take immediate action to remediate any identified deficiencies.
- Cybersecurity phases
  - Identify, protect, detect, respond, and recover
- Support your institution's efforts
- Know your cybersecurity leads

RESOURCES

- Final Rule
- Dear Colleague Letters: GEN 16-12, GEN 15-18
- Electronic Announcement: *Protecting Student Information – Compliance with CUI and GLBA*
- FSA Handbook
- NIST SP 800-171

QUESTIONS?

PRESENTERS

Brandon S. Sherman
BSherman@maynardcooper.com
202.868.5925

Starr Drum
SDrum@maynardcooper.com
205.254.1852

Roger Swartzwelder
RSwartzwelder@maynardcooper.com
202.868.5929

THANK YOU