Revised GLBA Safeguards Rule

MAACS

February 24, 2022

Brandon Sherman and Adam Griffin

PRESENTERS

- **Brandon Sherman** - Maynard Cooper & Gale
- **Adam Griffin** - Maynard Cooper & Gale

PRESENTER BACKGROUND

Brandon Sherman

- Practice and Experience
  - Previous Experience: Senior Counsel to the Deputy Secretary
  - Advises institutions on meeting U.S. Department of Education cybersecurity requirements
  - Counsels clients on the rules and procedures related to federal financial aid, accreditation, Title IX, and transactional issues
- Contact Information
  - Bsherman@MaynardCooper.com
  - 202-868-5925

PRESENTER BACKGROUND

Adam Griffin

- Practice and Experience
  - Cybersecurity and compliance
  - Work as breach coach to counsel organizations through incidents
- Contact Information
  - AGriffin@maynardcooper.com
  - 205-415-4903

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.*

OUR CLIENT BASE

KEY INDUSTRIES SERVED

- Admiralty and Maritime
- Automotive and Aerospace
- Agriculture
- Autonomy and Robotics Systems
- Banking and Financial Services
- Defense and Aviation
- Energy, Utilities, and Natural Resources
- Fintech
- Governmental Entities
- Health Care
- Higher Education
- Industrial, Manufacturing, and Distribution
- Insurance
- Internet of Things (IoT)
- Life Sciences
- Manufacturing
- Medical Devices
- Non-Profit
- Outdoor Products
- Personalized Medicine and Genomics
- Real Estate
- Senior Living and Long-Term Care
- Sports and Entertainment

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**

NATIONALLY RANKED CYBERSECURITY & PRIVACY PRACTICE

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**.

RECENT CYBER TRENDS

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic

MAYNARD COOPER GALE

INSTITUTIONS ARE **TARGETED** BY CYBER CRIMINALS

- They collect and store a high volume of **sensitive data** (financial, health, PII).
- The **operational impact** of a cyber attack could be crippling. . . and criminals know this.
- Without critical systems, you may be unable to:
  - Hold classes
  - Process payments
  - Pay employees
  - Process grades
  - Communicate with students and faculty
- Increased vulnerabilities due to **COVID-19**.

COMMON CYBER INCIDENTS

- Target student **PII** to resell on the black market.
- Encrypting school system data for **ransom**.
- Target student **direct deposit information** to redirect financial aid reimbursements to attacker bank accounts.
- IRS impersonation scam that appears to primarily target educational institutions.

ELECTRONIC ANNOUNCEMENT

- GENERAL-22-02 *StopRansomware.gov website*
  - The Federal Government launched a website to help public and private organizations defend against the rise in ransomware cases. StopRansomware.gov.
  - StopRansomware.gov is an interagency resource that provides FSA partners and stakeholders with ransomware protection, detection, and response guidance that they can use on a single web.
  - FSA encourages IHEs to use this new website to understand the threat of ransomware, mitigate risk, and know what steps to take in the event of an attack.

  Link to the Electronic Announcement

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 about 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.

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."

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**.

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 from step b 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
- The SAIG Enrollment Agreement requires schools to **immediately notify** the Department of a breach
- GLBA compliance requirement
- Institutions' **point of contact** 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.

GLBA OVERVIEW

- Previously, GLBA required a financial institution to:
  - Develop, implement, and maintain a **written information security program**;
  - Designate the employee(s) responsible for **coordinating** the information security program;
  - Periodically **evaluate and update** your school's security program;

CURRENT RULE

- Previously, GLBA required a financial institution to:
  - **Identify and assess** risks to customer information; and
  - Select appropriate **service providers** that are capable of maintaining appropriate safeguards.

RULEMAKING

- The FTC is required to periodically review all of its rules and guidance.
- On September 7, 2016, the FTC published a Request for Public Comment.
  - The FTC requested public comments on "the economic impact and benefits of the Rule; possible conflict between the Rule and state, local, or other federal laws or regulations; and the effect on the Rule of any technological, economic, or other industry changes."
- The FTC received 28 public comments, including by the American Council on Education.

FINAL RULE

- 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 "that strengthens 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

- Statement by Chair Lina M. Khan
  - "The amendments adopted today require financial institutions to develop information security programs that can meet the challenges of today's security environment."
  - "Despite the increasing sophistication of cyberattacks, many businesses continue to offer inadequate security."
- Dissenting statement by Commissioners Joshua Phillips and Christine Wilson
  - "[T]he new prescriptive requirements could weaken data security by diverting finite resources towards a check-the-box compliance exercise and away from risk management tailored to address the unique security needs of individual financial institutions."

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 based on the risk assessment and how the information security program will address the financial institution's risk.

KEY CHANGES

- Incident response plan:
  - The Final Rule requires financial institution 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 to plan following security event

KEY CHANGES

- The Final Rule requires financial institutions to design and implement **safeguards to control risks**, including by:
  - Implementing and periodically reviewing access controls, including technical and physical controls;
  - Encrypting all customer information held or transmitted by a financial institution both in transit over external networks and at rest;
  - Identifying and managing the data, personnel, devices, systems, and facilities that enable a financial institution to achieve business purposes in accordance with their relative importance to their business objectives and risk strategy;

KEY CHANGES

- The Final Rule requires financial institutions to design and implement safeguards to control risks, including by (cont'd):
  - Implementing **multi-factor authentication** for any individual accessing any information system;
  - Developing, implementing, and maintaining procedures for the **secure disposal of customer information**; and
  - Implementing policies, procedures, and controls designed to **monitor and log the activity** of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

KEY CHANGES

- Financial institutions must designate **a qualified individual responsible** for overseeing and implementing a financial institutions information security program and enforcing their information security program.
  - Qualifications will depend upon the size and complexity of a financial institution's information system and the volume and sensitivity of the customer information that the financial institution possesses or processes.
  - A Chief Information Security Officer title is not required.

KEY CHANGES

- The qualified individual must submit an **information security report** in writing, regularly and at least annually, to a financial 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 management's responses thereto, and recommendations for changes in the information security program.

KEY CHANGES

- **Training requirements** include:
  - Providing personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;
  - Utilizing qualified information security personnel employed by the financial institution or service provider sufficient to manage information security risks and to perform or oversee the information security program;
  - Providing information security personnel with security updates and training sufficient to address relevant security risks; and
  - Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

KEY CHANGES

- Expands the definition of “financial institution” to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities.
  - This change adds “finders”—companies that bring together buyers and sellers of a product or service within the scope of the Rule.

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

- Small businesses
  - The Final Rule exempts financial institutions that collect information about fewer than 5,000 consumers from the:
    - 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 financial institutions notify the FTC of detected security events under certain circumstances.

OTHER ISSUES

- The FTC declined to incorporate or reference NIST standards.
- Institutions of higher education continue to be considered "financial institutions."

IMPACT IN HIGHER EDUCATION

- The U.S. Department of Education will require compliance with the revised Rule.
- Changes will be incorporated into your annual compliance audit.
- Costs of compliance are borne by the institution

GLBA NON-COMPLIANCE

- FTC
  - Fines
  - Consent agreement

GLBA NON-COMPLIANCE

- U.S. Department of Education
  - Loss of access to FSA systems
  - Initiation of a Termination Action
  - Denial of an Open Recertification Action
  - Initiation of a Limitation Action
  - Imposition of a Fine action
  - Placement on HCM

FUTURE COMPLIANCE CONSIDERATIONS

- NIST SP 800-171 compliance
- New cybersecurity program at the U.S. Department of Education

NEXT STEPS

- Recommendations for institutions in light of the Final Rule:
  - Conduct a holistic risk assessment.
  - Ensure the board of directors and executive leadership is familiar with the Final Rule's requirements and understands the need to implement new measures.

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

Adam Griffin
AGriffin@maynardcooper.com
205.415.4903

MAYNARD
COOPER GALE

THANK YOU

MAYNARD
COOPER GALE