MAYNARD
COOPER GALE

Client Alert: Gramm-Leach Bliley Act (GLBA) Amended Safeguards Rule

The Federal Trade Commission ("FTC") considers institutions of higher education ("IHE") participating in federal financial aid programs authorized under the Higher Education Act, as amended, to be covered financial institutions under the Gramm-Leach Bliley Act. The FTC's oversight activities are carried out in accordance with the Safeguards Rule ("Rule"). 16 C.F.R. Part 314.

This fall, the FTC, issued an amended Rule. In sum, the amended Rule contains five main modifications to the existing Rule:

- It adds provisions designed to provide financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program.
- It adds provisions designed to improve the accountability of "financial institutions' information security programs, such as by requiring periodic reports to boards of directors or governing bodies.
- It exempts financial institutions that collect less customer information from certain requirements.
- It expands the definition of "financial institutions" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities.
- It defines several terms and provides related examples in the Rule itself rather than incorporating them by reference.

Written Risk Assessment

The final Rule requires that each IHE prepare a written risk assessment. This assessment must include or address each of the following items:

(1) Criteria for evaluating identified risks faced by the financial institution;
(2) Criteria for the assessment of the confidentiality, integrity, and availability of the financial institution's information systems and customer protection; and
(3) 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.

Security Controls

The current Rule provides flexibility for institutions to design and implement safeguards to control the risks identified in the risk assessment. In contrast, the revised Rule requires financial institutions to design and implement safeguards to control risks, including by:

(1) Implementing and periodically reviewing access controls, including technical and physical controls;
(2) Encrypting all customer information held or transmitted by a financial institution both in transit over external networks and at rest;
(3) 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;
(4) Implementing multi-factor authentication for any individual accessing any information system;
(5) Developing, implementing, and maintaining procedures for the secure disposal of customer information; and
(6) 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.

Information Security Coordinator

Under the final Rule, IHEs 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.

Board of Directors Oversight

The final Rule includes a role for an institution's Board of Directors. Under the revised Rule, 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:

(1) The overall status of the information security program and the financial institution's compliance with the Rule; and
(2) 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.

Definition of a Financial Institution

In response to its initial proposals for amending the current Rule, the FTC received comments from several higher education organizations urging the FTC to revise the definition of a "financial institution" to exclude institutions of higher education. However, the FTC rejected those suggestions and continues to consider IHEs as "financial institutions."

Training Requirements

Under the revised Rule, training requirements include:

(1) Providing personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;
(2) 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;
(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and
(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

Service Providers

Under the current Rule, financial institutions must take reasonable steps to select service providers capable of maintaining appropriate safeguards for customer information. The revised Rule goes one step further. Financial institutions must now oversee service providers by requiring financial institutions to periodically assess service providers based on the risk they present and the continued adequacy of their safeguards.

Effective Date
This revised Rule is effective January 10, 2022. However, key provisions, including the appointment of a qualified individual and conducing a written risk assessment, will be effective December 9, 2022.

As a reminder, as part of an institution's Program Participation Agreement, an institution agrees to comply with:

> The Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), as required by the Gramm-Leach-Bliley (GLB) Act, P.L. 106-102.

In addition to the Safeguard Rule, the U.S. Department of Education has informed IHEs and their third-party services of the Department's plan to require compliance with

National Institute of Standards and Technology Special Publication 800–171 Rev. 2, Controlled Unclassified Information in Nonfederal Systems (NIST 800–171 Rev. 2).

We recommend that IHEs that fall short of the updated requirements assess their current gaps and immediately begin to design and implement plans in order to close those gaps. We are available to provide any advice or assistance you may need.

Maynard Cooper is a full-service firm with attorneys experienced in all regulatory and operational aspects of higher education, including federal and state oversight, accreditation, employment and benefits issues, transactions, corporate and finance matters, and real estate concerns.

Brandon Sherman advises postsecondary institutions, accrediting agencies, and education investors on matters pertaining to federal financial aid eligibility, accreditation, cybersecurity, and Title IX.

Roger Swartzwelder advises regionally and nationally accredited institutions of higher education regarding legal, regulatory, accreditation, and transaction matters.