MEMORANDUM

TO: MCCCD College Presidents and CIOs

FROM: Melissa Flores, Interim General Counsel and Dr. Mark Koan, CIO

DATE: May 17, 2022

RE: Gramm-Leach-Bliley Act Safeguards Rule: More Information from the FTC

The Rule was promulgated under the Gramm-Leach-Bliley Act which, in part, requires the FTC to issue rules setting forth standards that financial institutions must implement to safeguard certain information. The Rule applies to customer information held by non-banking financial institutions and "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of [that information]."

THE AMENDMENTS

The amendments to the Rule became effective Jan. 10, 2022, although some of the most important provisions are not effective until Dec. 9, 2022. A summary provided by the FTC provides:

- More guidance on how to develop and implement specific aspects of an overall information security program.
- New provisions to improve the accountability of information security programs.
- New terms and examples.

WHAT'S NEW

Section 314.2 – Seven New Definitions.

As mentioned above, most of the defined terms are newly added to this section but not new to the Rule because they were previously cross-referenced to their definitions in the Privacy Rule. Following are the seven new terms, and one that has been modified:

1. Authorized User: This new term "means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data."
2. Encryption: This new term "means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material."
3. Financial Institution: This term has been modified to include "any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities. . ." (emphasis added). It specifically applies to "[a] company acting as a finder in bringing together one or more

buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate is a financial institution because acting as a finder is an activity that is financial in nature or incidental to a financial activity listed in 12 CFR 225.86(d)(1)."

4. Information Security Program: This new term "means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information."
5. Multi-Factor Authentication: This new term "means authentication through verification of at least two of the following types of authentication factors: (a) Knowledge factors, such as a password; (b) Possession factors, such as a token; or (c) Inherence factors, such as biometric characteristics."
6. Penetration Testing: This new term "means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems."
7. Security Event: This new term "means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form."

Section 314.5 – Effective Date. This section identifies certain provisions of § 314.4 that are not effective until Dec. 9, 2022, as described below.

Section 314.6 – Exceptions. This "small business" section identifies certain provisions of § 314.4 that "do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers." This does not apply to MCCCD.

WHAT'S HOT

Section 314.4 – Elements. This section has been completely overhauled, and now explains with specificity the elements, new and old, that must be included in an information security program. Except where indicated, these elements must be incorporated by Dec. 9, 2022. In summary, the elements checklist includes:

1. A single "qualified individual" designated to oversee, implement, and enforce the information security program. Previously, the program could be coordinated by a designated employee or employees.
2. An information security program based on a risk assessment. This is a current requirement, as well as the need to periodically perform additional risk assessments. However, effective Dec. 9, 2022, the risk assessment must include:
    a. Criteria for the evaluation and categorization of identified security risks or threats;
    b. Criteria for the assessment of the confidentiality, integrity, and availability of information, including the adequacy of the existing controls in the context of the identified risks or threats; and

    c. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.
3. Safeguards designed to control identified risks through:
    a. Access controls, including technical and physical controls, to authenticate and limit access;
    b. Identification and management of data, personnel, devices, systems, and facilities;
    c. Encryption of all customer information held or transmitted;
    d. Secure development practices and security testing for applications used for transmitting, accessing, or storing customer information;
    e. Multi-factor authentication for any individual accessing any information system;
    f. Procedures for the secure disposal of customer information no later than two years after the last date the information is used;
    g. Procedures for change management;
    h. Policies, procedures, and controls to monitor and log the activity of authorized users and detect unauthorized access, use or tampering.
4. Regular testing and monitoring of the safeguards' effectiveness. This general requirement is currently in effect, but new requirements effective Dec. 9, 2022, are:
    a. Continuous monitoring or annual penetration testing (CISA scans may provide continuous monitoring–more information to come); and
    b. Vulnerability assessments.

    Policies and procedures that include:

    a. Security awareness training;
    b. Use of qualified information security personnel to manage risks and oversee the program;
    c. Security training and updates to address risks; and
    d. Verification that information security personnel maintain current knowledge of changing information security threats and countermeasures.
5. Service provider oversight through:
    a. Selecting service providers capable of maintaining appropriate safeguards, which is a current requirement (Legal is reviewing whether the PSQS process meets this requirement);
    b. Requiring the safeguards by contract, which is also a current requirement (Legal is reviewing whether the Data Security Addendum meets this requirement); and
    c. Periodically assessing service providers based on the risk they present and the adequacy of their safeguards, effective Dec. 9, 2022.
6. A written incident response plan, with seven specific requirements, designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information.

7. A regular written report, prepared at least annually, by the qualified individual to the board of directors that includes the status of, and compliance with the information security program, and any related material matters.

COMPLIANCE

The elements described in § 314.4 are not new concepts and your college may already be compliant. However, because the elements are now far more specific and detailed than before, we recommend each college compare its elements to those of their own programs to ensure compliance, leaving time for compliance by Dec. 9, 2022.