ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
FEB. 8, 2023

# Amended rule expands data security requirements for financial institutions

■ **Michael Staszkiw and Anna Mercado Clark** SPECIAL TO THE RBJ


*Anna Mercado Clark*


*Michael Staszkiw*

On Dec. 9, 2021, the Federal Trade Commission (FTC) amended the Safeguards Rule to the Gramm-Leach-Bliley Act (GLBA), which may affect the responsibilities of businesses, including retailers and auto dealerships that provide financing, with regard to how they protect and maintain customers' nonpublic personal information.

These amendments expand the scope of the Safeguards Rule to apply to more types of entities and provide guidance on how to develop and implement specific aspects of an information security program. Compliance with these amendments can be confusing and overwhelming, especially for newly subjected entities that may not have the required policies and procedures in place.

Certain portions of the amendments were set to take effect on December 9, 2022; however, the FTC extended the deadline for compliance to June 9, 2023.

## BACKGROUND

Generally, GLBA regulates financial institutions and their management of nonpublic personal information, defined as "personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A). Under GLBA, financial institutions are required to comply with the FTC's Privacy Rule and the Safeguards Rule.

The Privacy Rule establishes a standard for privacy notices that financial institutions must provide to consumers that describe, among other things, what information the financial institution collects, with whom it shares the information, how it protects or safeguards the information, and an explanation of how a consumer may opt out of having their information shared through a reasonable opt-out process.

Meanwhile, the accompanying Safeguards Rule requires financial institutions to maintain certain security controls to protect the confidentiality and integrity of customer information — any record (paper or electronic) that contains nonpublic personal information about a customer of a financial institution. 16 C.F.R. § 314.2(d).

## EXPANDED DEFINITION OF 'FINANCIAL INSTITUTION'

The amendments expand the definition of financial institution to include entities "engag[ed] in an activity that is financial in nature or incidental to" financial activities. 16 C.F.R. § 314.2(h)(1). For example, the amendments explain that a finder, who is someone that brings together buyers and sellers of any product or service for a transaction, is a financial institution because "acting as a finder is an activity that is financial in nature or incidental to a financial activity." 16 C.F.R. 314.2(h)(2)(xiii). Thus, companies that offer third-party financing, such as auto dealerships or retail stores, may now be required to comply with the Safeguards Rule.

## DATA SECURITY OBLIGATIONS CREATED BY THE AMENDMENTS

The existing Safeguards Rule requires covered financial institutions to develop, implement and maintain a written comprehensive information security program that contains administrative, technical and physical safeguards to maintain the security and integrity of customers' information. The amendments expand on this obligation and provide a comprehensive list of safeguards and controls that a covered financial institution may want to include in its information security program. A covered financial institution should consult with counsel as to which safeguards it should include in its information security program and how best to implement those items to meet the particular needs of the business. Below is a non-exhaustive list of the safeguards and controls added by the amendments:

**Designating a qualified individual:** The current Safeguards Rule requires a covered financial institution to designate an employee to coordinate its information security program (Qualified Individual). The amendments allow covered financial institutions to now outsource this role through an affiliate or third-party service provider, in which case the financial institution

ROCHESTER BUSINESS JOURNAL

is subject to additional safeguards. The amendments also impose obligations on the Qualified Individual to report, at least annually, to the board of directors or governing body of the financial institution on the overall status of the information security program and any material matters related to the program and any recommended changes.

**Risk assessments:** The existing Safeguards Rule requires a covered financial institution to conduct periodic risk assessments and regularly test or otherwise monitor the effectiveness of the safeguards. The amendments list new specifications that the risk assessment should include, such as criteria for the evaluation and categorization of identified risks or threats the entity faces; criteria for the assessment of the confidentiality, integrity and availability of information systems and customer information; and requirements that describe how identified risks will be mitigated, and how the information security program will address the risks. The covered financial institution should then evaluate and adjust its information security program in light of the risk assessment's results. 16 C.F.R. § 314.4(g).

**Access controls:** A covered financial institution should implement and review access controls to customers' information. Id. § 314.4(c). Covered financial institutions should have in place procedures and controls to monitor and log the activity of authorized users and detect unauthorized access or use of customer information. Id. § 314.4(c)(8).

Encryption: A covered financial institution should encrypt customer information in transit or at rest. To the extent that encryption is not feasible, the covered financial institution may secure customer information using an effective alternative provided such alternative is reviewed and approved by the Qualified Individual. Id. § 314.4(c)(3).

**Multi-factor authentication:** A covered financial institution should implement multi-factor authentication before any individual may access its information systems. Id. § 314.4(c)(5).

**Disposal of customer information:** A covered financial institution should develop, implement and maintain procedures to securely dispose of customer information (electronic and paper) no later than two years after such information is last used, unless such information is necessary for business operations or otherwise required by law or regulation. Id. § 314.4(c)(6).

**Penetration testing and vulnerability assessments:** While the existing Safeguards Rule requires a covered financial institution to regularly test or monitor the safeguards it has in place, the amendments clarify that such financial institution should conduct annual penetration tests of its information systems and vulnerability scans every six months to identify publicly known security vulnerabilities that may exist. Id. § 314.4(d).

**Employee training:** Security awareness training should be provided to employees and information security personnel to address any risks identified by the covered financial institution's risk assessment. Additionally, information security personnel should be provided with security updates and training to address relevant information security risks. Id. § 314.4(e).

**Oversee service providers:** The existing Safeguards Rule requires a covered financial institution to take certain steps to oversee its service providers. 16 C.F.R. § 314.4 (f). The amendments also suggest a covered financial institution should conduct periodic assessments of service providers "based on the risk they present and the continued adequacy" of their own safeguards regarding customer information. Id. § 314.4(f)(3).

**Develop an incident response plan:** Covered financial institutions should also establish a written incident response plan designed to respond to and recover from any security event that "materially affect[s] the confidentiality, integrity, or availability of customer information." Id. § 314.4(h).

## ARE THERE ANY EXCEPTIONS?

Financial institutions that maintain customer information concerning less than 5,000 consumers may be exempt from the following amendment data security obligations:

- The additional risk assessment criteria
- Having to conduct penetration tests and vulnerability scans
- Having an incident response plan
- The Qualified Individual having to report to its board of directors

However, a covered financial institution that qualifies for the exceptions should still be aware that other data security state laws may still apply. For example, New York's § 899-bb of New York's SHIELD Act, which imposes similar, but distinct, obligations on businesses to develop, implement and maintain reasonable safeguards to protect the confidentiality and integrity of New York residents' private information.

## WHAT CAN BUSINESSES DO?

To prepare for these amendments to take full effect, businesses may want to consider:

- The applicability of the Safeguards Rule to their organization
- The obligations they may have under the Safeguards Rule
- Contacting counsel to establish or update their strategy for complying with the Safeguards Rule, which may include reviewing and revising their policies and procedures

*Michael R. Staszkiw, CIPP/US, is an attorney at Phillips Lytle LLP and member of the firm's Data Security & Privacy Team. He can be reached at mstaszkiw@phillipslytle.com or (585) 238-2044. Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy Practice Team. She can be reached at aclark@phillipslytle.com or (585) 238-2000 x6466.*