Overview

Federal Trade Commission (FTC) Safeguards Rule

Dan Pepper, Elyssa Diamond, and Esther Clovis, Norton Rose Fulbright US LLP

Bloomberg Law

Federal Trade Commission (FTC) Safeguards Rule

Contributed by Dan Pepper, Elyssa Diamond, and Esther Clovis, Norton Rose Fulbright US LLP

In 2021, the FTC amended its Standards for Safeguarding Customer Information, 16 C.F.R.Part 314, otherwise known as the "Safeguards Rule." Promulgated in response to § 501 of the Gramm-Leach-Bliley Act of 1999 (GLBA), which obligates the federal agencies that regulate financial institutes to establish "appropriate standards . . . relating to administrative, technical, and physical safeguards" of nonpublic personal information, the Safeguards Rule ensures that covered financial institutions protect the security of customer information. The following overview summarizes key revisions to the Safeguard Rule's applicability and information security requirements, fully effective June 9, 2023, as well as requirements governing service provider contracts and data retention.

Revisions to Applicability & Information Security Requirements

The amended Safeguards Rule maintains the main elements of the Rule as originally published in 2003—it requires a designated program coordinator, someone to oversee service providers, a comprehensive risk assessment, adequate safeguards and regular audits, and adjustments to the information security program as needed. However, the 2003 Safeguards Rule was more flexible, while the amended version outlines more technical requirements necessary for compliance. The key changes to the Rule as amended are as follows:

- A non-exhaustive list of covered entities, including:
    - Mortgage lenders;
    - Payday lenders;
    - Finance companies;
    - Mortgage brokers;
    - Account servicers;
    - Check cashers;
    - Wire transferors;
    - Collection agencies;
    - Credit counselors and other financial advisors;
    - Tax preparation firms;
    - Non federally insured credit unions; and
    - Investment advisors that aren't required to register with the SEC.
- A single "Qualified Individual."
    - While the 2003 Rule required that a covered entity designate one or more employees to coordinate the information security program, the rule as amended requires that the program is run by a single Qualified Individual, who can be an employee, affiliate, or service provider. If the covered entity appoints a non-employee as the Qualified Individual, the covered entity will still be ultimately responsible for compliance with the Safeguards Rule.
- A written risk assessment.
    - The amended Safeguards Rule requires that the risk assessment that the security program is based on be written. The goal of the risk assessment is to identify reasonably foreseeable internal and external risks to the security of customer information and it should include the following elements:

1. Criteria for the evaluation and categorization of identified security risks faced by the covered entity
2. Criteria for the assessment of the integrity of the covered entity's information systems. In light of the identified risks, the covered entity should consider the adequacy of existing controls.
3. A description of how the identified risks will be mitigated or accepted and how the information security program will address the risks.

    - In addition, the covered entity should periodically perform additional risk assessments to reexamine the risks and reassess the sufficiency of the safeguards in place to control them.

- Additional safeguards.
    - The 2003 Rule requires that a covered entity implement safeguards to control the risks identified through the risk assessment. The amended Rule builds on this safeguard requirement by adding technical and physical limitations on who can access customer data, data encryption, and multi-factor authentication, among other security measures.
- Penetration testing.
    - The amended Rule requires either continuous monitoring of information systems, or annual penetration testing and vulnerability assessments at least every six months.
- Personnel training.
    - Covered entities must provide personnel with security awareness training and other trainings to address relevant security risks and current information about security threats.
- Incident response plan.
    - Covered entities must implement a written incident response plan that addresses a number of areas such as internal processes for responding to a security event and defined roles, responsibilities, and levels of decision-making authority.
- Board reports.
    - The designated Qualified Individual must provide the board of directors or equivalent governing body with a written report, at least annually, addressing the covered entity's information security program.

Contractual Requirements

The Safeguards Rule requires financial institutions to oversee their service providers' compliance with the Safeguard Rule by contracting with them to do so. 16 C.F.R. § 314.4(f). These contracts must require service providers with access to customer information to take appropriate measures to prevent the unauthorized access or use of customer information where such access or use could cause substantial harm or inconvenience to any customer. 16 C.F.R. § 314.3(b)(3).

Note that financial institutions that are regulated by federal agencies other than the FTC must also require service providers, by contract, to implement appropriate measures designed to meet the objectives of the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Guidelines), 12 C.F.R. Part 364, Appendix B. For additional information on the Guidelines, see Overview – IT Security & Cloud Guidance for Financial Institutions.

Data Retention

The GLBA does not specify a record or data retention period. However, under the Safeguards Rule, entities subject to the GLBA must securely dispose of customer information no later than two years after the most recent use of that data to serve the customer unless the entity's retention of customer information falls under one of two exceptions: 1) the entity has a legitimate business need or legal requirement to hold onto the data, or 2) disposal of the customer's information is not feasible because of the manner in which the information is maintained. 16 C.F.R. § 314.4(c)(6)(i); FTC Press Release, "FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches," (Oct. 27, 2021).

Subject entities must also periodically review their data retention policies to minimize the unnecessary retention of data. 16 C.F.R. § 314.4(c)(6)(ii).