



FTC Amendments Affecting Financial Institutions

Articles / Publications

04.14.2022

As of January 10, 2022, the FTC's amendments to the Safeguards Rule ("Amendments") went into effect, 16 CFR Part 314; RIN 3084-AB35, Standards for Safeguarding Customer Information. The Amendments apply to financial institutions, not only banks. The Amendments include five (5) primary modifications to the Safeguards Rule. These modifications generally relate to heightened information security requirements and expanding the definition of "financial institution."

The Gramm Leach Bliley Act ("GLBA") provides a framework for regulating the privacy and data security practices of a broad range of financial institutions. Among other things, GLBA requires financial institutions to provide customers with information about the institutions' privacy practices and their opt-out rights. It requires financial institutions to implement security safeguards for customer information.

GLBA required the FTC and other federal agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information. Accordingly, the FTC promulgated the Safeguards Rule in 2002. The Amendment discussed herein updates the Safeguards Rule.

A financial institution is any institution whose business involves engaging in financial activities. For example, financial institutions include:

- Retailers that extend credit by issuing their own credit card directly to consumers;

RELATED PROFESSIONALS

Elizabeth B. Shirley, CIPP/US, CIPM

RELATED CAPABILITIES

Cybersecurity & Data Privacy

Financial Services

FTC Amendments Affecting Financial Institutions

- Personal property or real estate appraisers;
- Automobile dealerships that, as a regular part of business, lease automobiles on a non-operating basis for longer than 90 days;
- Career counselors that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company;
- Businesses that print and sell checks for consumers, either as their sole business or as one of their product lines;
- Businesses that regularly wire money to and from consumers;
- Check cashing businesses;
- Accountants or other tax preparation services that are in the business of completing income tax returns;
- Businesses that operate a travel agency in connection with financial services;
- Entities that provide real estate settlement services;
- Mortgage brokers;
- Investment advisory companies and credit counseling services;

See 16 CFR § 313.3(k)(1) & (k)(2) (emphasis added). The Amendments broaden the definition of “financial institution” to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. More specifically, the Amendments include as examples of financial institutions companies acting as finders in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate.

This broad definition of financial institutions is subject to heightened information security standards pursuant to the Amendments. While the Safeguards Rule required financial institutions to undertake a risk assessment and develop and implement safeguards to address identified risks, the Amendments set out criteria for what the risk assessment must include and requires that the risk assessment be in writing. The Amendments require that financial institutions address access controls, data inventory and classification, encryption, secure development practices, authentication, information disposal procedures, change management, testing, and incident response. The Amendments further add mechanisms designed to ensure the required employee training and oversight of services providers.

Additionally, the Amendments add requirements to improve accountability of financial institutions’ information security programs. They require the designation of a single Qualified Individual as the employee responsible for the information security program. The Amendments also require periodic reports to boards of directors or governing bodies to provide senior management with better awareness of the financial institutions’ information security programs. This requirement is to ensure that the information security programs will received the required resources, such as funding, and be able to protect consumer information.

FTC Amendments Affecting Financial Institutions

The Amendments exempt financial institutions that collect information on fewer than 5,000 consumers from the requirements of a written risk assessment, incident response plan, and annual reporting to the board of directors. Finally, the Amendments include an administrative revision to add several definitions and related examples (including “financial institution” in the Safeguards Rule, set out above), rather than incorporate them by reference from the related FTC rule, the Privacy of Consumer Financial Information Rule, 16 CFR 313. The goal was to make the Safeguards Rule more self-contained.

The Amendments reflect an increased focus on protecting the personal information – and specifically financial information – of businesses that collect, use, and store such information on a regular basis. Companies in the financial sector may be affected by the scope and requirements in the Amendments, and they should review their operations and collection, use, and storage of personal, financial information to ensure that they are compliant.