SpencerFane®

Whoa, My Business is a "Financial Institution" under the FTC's Safeguards Rule? Now What?

The Federal Trade Commission's (FTC) Standards for Safeguarding Customer Information (Safeguards Rule) was promulgated under the Gramm-Leach-Bliley Act (GLBA) with the intent to require financial institutions to develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.[1]

Traditional financial institutions (such as banks and credit unions) are very familiar with the GLBA and the requirements under the GLBA for the protection and security of customer information. However, because of the increase in new technologies that have enabled a variety of businesses to offer new services that may have some financial aspects, we are seeing regulators extending many of the compliance obligations once applicable only to traditional financial institutions to non-traditional "financial institutions."

In short, the Safeguards Rule requires non-bank financial institutions to develop, implement, and maintain a comprehensive information security program to keep their customers' information safe. None of this sounds surprising, right? But wait, is your business considered a "financial institution" under the Safeguards Rule? You may be surprised.

The Safeguards Rule applies to financial institutions subject to the FTC's jurisdiction and that aren't subject to enforcement authority of another regulator under section 505 of the GLBA.[2] The Safeguards Rule defines a business as a "financial institution" if the "business is engaging in an activity that is financial in nature or incidental to such financial activities . . ."[3]

So, what types of businesses come under this broader "financial institution" definition? Let's take a look:

- A retailer that extends credit by issuing its own credit card directly to consumers;
- An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days;
- A personal property or real estate appraiser;
- A career counselor 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;
- A business that prints and sells checks for consumers, either as its sole business or as one of its product lines;
- A business that regularly wires money to and from consumers;
- A check cashing business;
- An accountant or other tax preparation service;
- A business that operates a travel agency in connection with financial services;
- An entity that provides real estate settlement services;
- A mortgage broker;
- An investment advisory company and a credit counseling service; or
- 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.[4]

Surprising, right? By the way, the mandatory compliance date was June 9, 2023. If your business is a financial institution under the Safeguards Rule, the business needs to (quickly) do the following:[5]

- Conduct an initial risk assessment to identify internal and external risks to the security, confidentiality, and integrity of customer information.
- Develop, implement, and maintain a comprehensive written information security program based on the risk assessment, which should contain administrative, technical, and physical safeguards appropriate for the size and complexity of the business, the nature and scope of its activities, and the sensitivity of its customers' information.

- Designate a qualified individual responsible for implementing and enforcing the program.
- Regularly test or otherwise monitor the effectiveness of the safeguards' controls.
- Implement policies and procedures to ensure that personnel are able to enact the information security program.
- Oversee service providers by selecting and retaining only capable providers while requiring them to implement and maintain appropriate safeguards.
- Update the program on an ongoing basis.
- Establish a written incident response plan.
- Require the qualified individual to report, in writing, to the business' board of directors or equivalent governing body.[6]

This blog post was drafted by Shelli Clarkston, an attorney in the Spencer Fane Kansas City, Missouri office. For more information visit www.spencerfane.com.

[1] 16 CFR § 314.1(a)

[2] https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

[3] 16 CFR § 314.1(b)

[4] 16 CFR § 314.2(h)

[5] See the complete list of requirements in 16 CFR § 314.4.

[6] 16 CFR § 314.4.