Client Alert: GLBA Compliance

FTC Makes Significant Additions to the GLBA Safeguards Rule

By:Kevin S. Olson
February 01, 2023

Last year the Federal Trade Commission (FTC) released a number of important additions to the Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA). The Safeguards Rule requires covered financial institutions to maintain a comprehensive information security program to protect consumer information. Originally, the Safeguards Rule allowed for greater flexibility in designing a security program, but the updates impose more granular requirements that businesses must implement to remain in compliance.

Covered entities are now required to have a "qualified individual" responsible for managing the information security program, who must also submit annual reports to the board of directors regarding the security program. In addition, the updated Safeguards Rule adds criteria to be evaluated in risk assessments, which are now required to be written and conducted periodically.

As for the specific requirements, covered entities must now implement a number of specific safeguards, including:

- Access controls;
- Encryption;
- Secure app development practices;
- Multi-factor authentication;
- Data deletion and periodic review of retention policies;
- Change management procedures;
- Continuous monitoring, or periodic penetration testing and vulnerability assessments;
- A written incident response plan;
- Employee training; and
- Periodic review of risks posed by service providers.

In addition, the updated rule adds "finders" to the list of "financial institutions" that are covered as entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities.

Originally scheduled to go into effect in December 2022, the FTC has delayed the effective date of many of the more onerous provisions of the updated Safeguards Rule to **June 9, 2023**. Such provisions include appointing a qualified individual, annual reporting, conducting written risk assessments, and having a written incident response plan. Other aspects of the new Safeguards Rule which mandate periodic risk assessment, monitoring of information systems,

and general oversight of service providers went into effect in early 2022. The rule also includes a small business exception for certain requirements. The exception applies to covered entities handling the information of fewer than 5,000 consumers.

If you have questions about the updated Safeguards Rule or any other data protection matters, please contact Kevin Olson, Faith Kasparian, Ann O'Rourke, or Ryan Perry.