Safeguards Rule Compliance Deadline Extended by FTC

On Nov. 15, 2022, the Federal Trade Commission (FTC) announced a six-month extension for businesses to comply with certain changes made to the Safeguards Rule (the Rule). The Rule is a portion of the 2002 Gramm-Leach-Bliley Act (GLBA), which sets out required standards for safeguarding customer information for covered financial institutions. “Financial institutions” is defined broadly and includes organizations beyond traditional finance companies, such as higher education, mortgage brokers, mortgage lenders and some automotive dealerships, to name a few.

In late 2021, the FTC issued new rules designed to protect customer financial information against cybersecurity threats. Many of these new rules were to go into effect on Dec. 9, 2022. However, with the extension, financial institutions subject to the Rule now have until June 9, 2023 to bring their security programs into compliance with certain updated changes. These changes are intended to strengthen the data security safeguards financial institutions must put in place to protect their customers’ personal information. Unlike the prior Rule, which required financial institutions to comply with general customer information security guidance, the new Rule is more prescriptive and requires implementation of precise security procedures and specific technology to protect customer information. The new requirements fall within three broad categories: (1) Implementing Policies, Procedures, and Technical Updates; (2) Personnel Requirements; and (3) Service Provider Requirements.

Some changes went into effect 30 days after the publication of the rule in the Federal Register in 2021, while the significant operational and technical modifications were to go into effect on Dec. 9, 2022. The modifications set to become effective in December of 2022 are the only sections of the Rule affected by the FTC’s six-month extension. Those sections include requirements that covered financial institutions:

- Designate a qualified individual to oversee their information security program;
- Develop a written risk assessment policy and perform such risk assessments;
- Limit and monitor who can access sensitive customer information;
- Encrypt all sensitive information;
- Train security personnel;
- Develop an incident response plan;
- Periodically assess the security practices of service providers; and
- Implement multi-factor authentication or another method with equivalent protection for any individual accessing customer information.

The FTC is extending the deadline, in part, based on reports that there is a shortage of qualified personnel to implement information security programs and that supply chain issues may lead to delays in obtaining necessary equipment for upgrading security systems.

While the extended deadline provides extra time for compliance, covered entities should not delay their compliance efforts, especially given the shortages mentioned above. Any covered financial institution should review its current practices to ensure that it has the requisite measures in place to be compliant with the new Rule.

For more information regarding the new Safeguards Rule, contact Amber Lawyer, CIPP/E, CIPP/US, Shannon Knapp, CIPP/US or any attorney in cybersecurity and data privacy practice.

**Special thanks to Associate Trainee Jared A. Joyce for assisting with researching and drafting this memo.*