SAUL EWING ARNSTEIN & LEHR LLP

ALERT

Cybersecurity and Privacy Practice

NOVEMBER 2021

FTC Amends Standards for Safeguarding Customer Information

Alexander (Sandy) R. Bilus

On October 27, 2021, the Federal Trade Commission ("FTC") issued a Final Rule amending the Standards for Safeguarding Customer Information (also known as the "Safeguards Rule"), 16 C.F.R. Part 314. The Safeguards Rule sets the standards for administrative, technical, and physical protections for customer information collected and used by all financial institutions that are subject to the FTC's enforcement authority under the Gramm-Leach-Bliley Act ("GLBA").

What You Need to Know:

- The Safeguards Rule applies to all financial institutions that are subject to the FTC's enforcement authority under the Gramm-Leach-Bliley Act.
- The amendments include an expanded definition of "financial institution," new requirements for information security programs, and exemption for smaller institutions.
- Financial institutions that are subject to the Safeguards Rule will want to update their risk assessment process and confirm that they have the required safeguards in place to protect customer information.

The FTC's Final Rule modifies the Safeguards Rule in several key ways:

- **Expanded definition of "financial institution."** Under the Final Rule, the definition of "financial institution" subject to the enforcement authority of the FTC is expanded to include entities that are "finders" – i.e., companies that bring together buyers and sellers of a product or service. Accordingly, the "financial institutions" that are subject to the FTC's enforcement authority now include, but are not limited to, mortgage lenders, "pay day" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders.
- **New requirements for information security programs.** Under the Final Rule, financial institutions must now consider specific criteria as part of their risk assessment process, including (1) criteria for the evaluation and categorization of identified security risks or threats, (2) criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information, including the adequacy of existing controls, and (3) requirements for describing how identified risks will be mitigated or accepted based on the assessment and how the information security program will address the risks. Such risk assessments also must now be in writing. The Final Rule also requires institutions to design and implement specific safeguards to control the identified risks, including: (1) access controls to permit access only to authorized users, (2) data inventory and classification according to importance to business objectives and risk strategy, (3) encryption of customer information both in transit and at rest, (4) secure

development practices for in-house developed applications, (5) multi-factor authentication, (6) procedures for secure disposal of customer information, (7) change management procedures, (8) activity monitoring and logging, (9) regular testing of the safeguards' effectiveness, and (10) a written incident response plan. The Final Rule also includes new mechanisms meant to ensure that employee training and oversight of service providers are effective.

- **New accountability for information security programs.** The Final Rule will require financial institutions to designate a single "Qualified Individual" who is responsible for oversight and implementation of the information security program. The Final Rule also requires that the Qualified Individual periodically report to the board of directors to help raise awareness and make it more likely that financial institutions will allocate appropriate resources for information security.
- **Exemptions for smaller institutions.** Financial institutions that collect information on fewer than 5,000 consumers are exempted from the Final Rule's new requirements of a written risk assessment, incident response plan, and annual reporting to the board of directors.

The key changes will become effective one year after the Final Rule is published in the Federal Register. The FTC's announcement of the Final Rule can be viewed here, and the Final Rule itself can be viewed here.

If you have questions about the Final Rule, you can contact the author of this article of any member of Saul Ewing Arnstein & Lehr's Cybersecurity and Privacy Group.

This alert was written by Alexander "Sandy" Bilus, Co-Chair of the Firm's Cybersecurity and Privacy Practice. Alexander can be reached at (215) 972-7177 or Alexander.Bilus@saul.com. This alert has been prepared for information purposes only.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.