FTC's Final Rule Expands the Safeguards Rule for Financial Institutions to Address Cybersecurity Risks and the Privacy of Consumer Data

Client Alert

11.17.21

What You Should Know

- The FTC has amended the Safeguards Rule for non-bank providers of financial products and services by issuing a Final Rule.
- The updates are intended to enhance the security of consumer financial information and the protection of related cyber-data and facilitate greater transparency.
- Covered financial institutions will be required to engage in proactive risk assessment procedures and to report periodically to boards of directors or other governing bodies.
- The timeline for compliance with various elements of the expanded Safeguards Rule ranges from 30 days to one year following publication of the Final Rule in the Federal Register.

By: James A. Robertson

On October 27, 2021, the Federal Trade Commission (FTC) issued updates to the Standards for Safeguarding Customer Information promulgated under the Gramm-Leach-Bliley Act (GLBA) - commonly referred to as the Safeguards Rule. The Safeguards Rule provides the FTC with enforcement authority to ensure that financial institutions, such as entities that offer consumers financial products or services including loans, financial guidance, investment advice and insurance, explain to their customers their information-sharing practices and efforts to safeguard sensitive data. Samuel Levine, Director of the FTC's Bureau of Consumer Protection, noted that "financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it" and that the FTC's amendments to the Safeguards Rule (referred to as the Final Rule) "detail common-sense

steps that these institutions must implement to protect consumer data from cyberattacks and other threats."

Who is Impacted

The Safeguards Rule applies to all entities that are "significantly engaged" in providing financial products or services, regardless of size. The Safeguards Rule does not apply to banks, but it does apply to entities including check-cashing businesses, payday lenders, mortgage brokers, non-bank lenders, personal property or real estate appraisers, professional tax preparers, courier services, and businesses such as credit reporting agencies and ATM operators that receive information about the customers of other financial institutions. In addition to developing their own safeguards, entities covered by the Safeguards Rule are responsible for taking steps to ensure that their affiliates and service providers comply with the safeguarding of the customer information in their care.

Safeguards Rule Requirements and Key Modifications Under the Final Rule

The existing Safeguards Rule requires all covered entities to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the entity's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

As part of its plan, each covered entity must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of its operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure the contract with service providers requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the entity’s business or operations, or the results of security testing and monitoring.

The Final Rule modifies the Safeguards Rule in five key ways:

1. It adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, authentication, and encryption
2. It adds provisions designed to improve the accountability of financial institutions’ information security programs, such as requiring that a qualified individual at covered institutions provide periodic reports to boards of directors or governing bodies.
3. It exempts financial institutions that collect less customer information from certain requirements.
4. It expands the definition of “financial institution” to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. This change adds “finders” (*i.e.* companies that bring together buyers and sellers of a product or service) within the scope of the Safeguards Rule.

5. It explicitly includes several definitions and related examples – including the definition of "financial institution" – rather than incorporating them by reference from the FTC's Privacy of Consumer Financial Information Rule. This modification makes the Safeguards Rule more self-contained and should facilitate a better understanding of its requirements.

In addition to the above key modifications, the Final Rule sets forth the following requirements for covered financial institutions:

- **Written Risk Assessment Plan.** Covered financial institutions must establish a comprehensive written risk assessment plan that identifies and evaluates risks to its systems, evaluates the adequacy of its existing controls for addressing these risks, and identifies how these risks can be mitigated.
- **Encryption of Customer Information at Rest and in Transit.** Covered financial institutions must encrypt all customer information in transit and at rest, subject to certain compensating control exceptions.
- **Penetrating Testing and Vulnerability Assessments.** Covered financial institutions must continuously monitor or conduct periodic penetration testing and vulnerability assessments to detect actual and attempted attacks on information systems. Vulnerability assessments must be performed at least once every six months.
- **Designation of Single Qualified Individual.** Whereas the current Safeguards Rule requires covered financial institutions to designate one or more employees to coordinate their information security program, the Final Rule requires that covered financial institutions designate a single "qualified individual" for that purpose. The Final Rules does not list any specific qualifications (such as level of experience or education) for that qualified individual.
- **Small Businesses.** The Final Rule exempts financial institutions that collect or retain information about fewer than 5000 individuals from the written risk assessment plan, incident response plan, and annual reporting requirements.
- **Service Providers.** The current Safeguards Rule requires covered financial institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and requires those service providers by contract to implement and maintain such safeguards. The FTC expands this requirement with the Final Rule and argues that "some high profile breaches have been caused by service providers' security failures." Therefore, the Final Rule requires that covered financial institutions periodically assess service providers "based on the risk they present and the continued adequacy of their safeguards." This ongoing oversight of service providers could include investigating red flags raised by service providers' practices or conducting periodic assessments to ensure that service providers are safeguarding and protecting information systems.

Timeline for Compliance

The expanded Safeguards Rule will go into effect on two separate occasions. The requirements focused on the designation of a single qualified individual, written risk assessment plans, annual penetration testing, biannual vulnerability assessment testing, periodic assessments of service providers, and written incident response plans will become effective one year after the Final Rule is published in the Federal Register. All other requirements of the Final Rule will be effective within 30 days following publication of the Final Rule in the Federal Register.

Of Further Note

In addition to the modifications to the Safeguards Rule outlined above, the FTC is also seeking public comment on whether to further amend the Safeguards Rule to require covered financial institutions to report certain data breaches and other security events to the FTC. The proposed amendment would require covered financial institutions to report a data breach affecting or reasonably likely to affect at least 1000 consumers. This notice would be provided via a form on the FTC's website within 30 days of discovery of the breach and would require certain specified disclosures. The FTC has announced that it will soon publish a supplemental Notice of Proposed Rulemaking, after which the public will have 60 days to submit comments.

Additional information regarding the provisions and applicability of the updated Safeguards Rule is available on the FTC's website here and here. Please contact the authors of this Alert with questions or to discuss your specific circumstances.

Related Attorneys

James A. Robertson

Partner

973.577.1784

Email