

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

### 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.

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:

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

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

#### **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