wiley

ALERT

FTC Releases Detailed Information Security Requirements and Proposes Breach Notification for Financial Institutions

October 29, 2021

On October 27, 2021, the Federal Trade Commission (FTC) announced revisions to its Safeguards Rule (Revised Safeguards Rule), which requires certain financial institutions to implement information security programs to protect consumer financial information. The FTC's Safeguards Rule covers a range of companies that engage in financial activities and are subject to the Gramm-Leach-Bliley Act (GLBA), including many online financial technology (fintech) companies, mortgage lenders, and companies otherwise involved in credit transactions, among others.

The FTC voted 3-2 along party lines to approve the Revised Safeguards Rule, with Commissioners Khan and Slaughter issuing a joint statement and Commissioners Phillips and Wilson releasing a dissenting statement. While the joint statement praised the Revised Safeguards Rule as an effort to "meet the challenges of today's security environment," the dissenting statement criticized the regulations as a "one-size-fits-all" approach to data security that may not be flexible enough to meet its goals.

The Revised Safeguards Rule will require, within 30 days of Federal Register publication, covered companies to implement periodic risk assessments, modify their information security programs based in part on those risk assessments, and regularly test system controls and safeguards with more specific requirements. Additionally, within a year of Federal Register publication, the Revised Safeguards Rule will require covered companies to maintain written incident response plans and implement specific security requirements including multifactor authentication, access controls, and encryption. In a

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Antonio J. Reynolds
Partner
202.719.4603
areynolds@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Practice Areas

Fintech

FTC Regulation

separate supplemental notice of proposed rulemaking (SNPRM), the FTC is also proposing to add reporting of security incidents to the FTC by covered companies within 30 days of discovery.

Altogether, the revised rule represents a more prescriptive regulatory approach similar to the New York Department of Financial Services' cybersecurity regulation, and it will require more detailed compliance efforts by companies covered by GLBA including many fintechs.

Scope of FTC's Safeguards Rule and Latest Rulemaking

Congress directed the FTC to promulgate the Safeguards Rule through the passage of the Gramm-Leach-Bliley Act in 1999, and the Safeguards Rule was implemented in an effort to protect consumer financial information. The Revised Safeguards Rule largely covers the same financial institutions covered under the existing rule, including:

- Mortgage lenders and brokers
- Payday lenders
- Finance companies
- Account servicers
- Check cashers
- Wire transferors
- Travel agencies (when operated in connection with financial services)
- Collection agencies
- Credit counselors and other financial advisors
- Tax preparation firms
- Non-federally insured credit unions
- Investment advisors not required to register with the Securities and Exchange Commission

The revised rule also covers entities acting as "finders" and exempts financial institutions with information on fewer than five thousand consumers from certain requirements.

The FTC announced proposed revisions to the Safeguards Rule through a request for public comment in March 2019. In July 2020, the agency held a workshop to examine the proposed changes to the Safeguards Rule. The workshop explored the practical application of the proposed revisions, as well as the costs and benefits to rule changes. The Revised Safeguards Rule adopts many of the proposals included in the 2019 request for comment and discussed at the workshop a year later. Some of those newly adopted proposals will take effect 30 days after Federal Register publication, while others will not be implemented until one year following publication.

Rules Effective 30 Days After Publication

The Revised Safeguards Rule requires covered financial institutions to, among other things, base their information security program on a periodic risk assessment and regular testing that is designed to detect actual and attempted attacks on, or intrusions into, information systems. Covered financial institutions are also required to modify their information security programs in accordance with periodic risk assessments.

Rules Effective One Year After Publication

Many additional security requirements go into effect one year after publication. For example, covered financial institutions will be required to:

- Require a "qualified individual" to oversee and implement the information security program;
- Require the designated "qualified individual" to regularly report in writing to the company board of directors or equivalent governing body;
- Implement access controls, encryption, multi-factor authentication, retention and disposal policies, and logging;
- Establish periodic security assessments for service providers; and
- Create written incident response plans.

Additionally, the rules that will take effect one year after publication include more specific requirements for periodic risk assessments. Specifically, the risk assessment must: (1) evaluate the categorization of identified security risks that the financial institution faces; (2) assess the confidentiality, integrity, and availability of information systems and customer information; and (3) describe how the identified risks will either be mitigated or accepted based on the risk assessment, and how the financial institution's information security program will address the risks. The Revised Safeguards Rule also requires that regular testing include penetration testing and vulnerability assessments.

Additional Proposed Changes.

The FTC is also seeking comment on further changes to the rule through a supplemental notice of proposed rulemaking (SNPRM). Specifically, the SNPRM proposes to add reporting of security incidents to the FTC by covered financial institutions within 30 days of discovery. Additionally, the notification would include (1) the name and contact information of the company reporting the incident; (2) a description of the type of information involved in the incident; (3) if possible to determine, the date or timeline of the event; and (4) a general description of the security event. Comments on the SNPRM will be due 60 days after publication in the Federal Register.

In light of these changes, covered companies will need to closely evaluate their security practices for compliance, and should consider weighing in on incident reporting provisions that have been issued for comment. Should you have any questions, please contact one of the authors.