wiley

ALERT

FTC Examines Proposed Amendments to the GLBA Safeguards Rule in Full-Day Workshop

July 15, 2020

On July 13, 2020, the Federal Trade Commission (FTC) held a workshop examining the proposed amendments to the Gramm-Leach-Bliley Act's (GLBA's) Safeguards Rule, which would expand the scope of companies covered by the Rule and mandate that covered entities take certain specific steps to secure customers' information, including encryption and multi-factor authentication.

A key goal of the workshop was to better understand the costs and benefits of the practices set forth in the proposed amendments. Topics of focus included (1) price models for specific elements of information security programs; (2) standards for security in various industries; (3) the availability of third party information security services aimed at different sized institutions; (4) information about penetration and vulnerability testing; and (5) the costs of, and possible alternatives to, encryption and multifactor authentication.

The proposed amendments have been criticized by two of the FTC's Commissioners, who have expressed concern that they are "overly prescriptive" and may "trad[e] flexibility for a costly one-size-fits-all approach," and have emphasized that "input from stakeholders [is] vital." The FTC is accepting comments through **August 12, 2020**, providing industry stakeholders with an additional opportunity to add to the evidentiary record that the FTC will consider in deciding whether to amend the Rule.

The Proposed Amendments Would Significantly Change the Safeguards Rule. The Safeguards Rule requires companies defined as "financial institutions" to develop, implement, and maintain a comprehensive information security program designed to insure the security and confidentiality of customer information, protect against

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Antonio J. Reynolds
Partner
202.719.4603
areynolds@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

FTC Regulation

Privacy, Cyber & Data Governance

anticipated threats or hazards to the security or integrity of that information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[1] The FTC adopted the Safeguards Rule on May 23, 2003 pursuant to the Gramm-Leach-Bliley Act (GLBA)[2] and no changes have been made to the Rule since its adoption. On March 5, 2019, the FTC announced a Notice of Proposed Rulemaking (NPRM) that proposed several amendments to the Safeguards Rule, including:

More Specific and Prescriptive Security Requirements. The NPRM proposes amending the Rule to include more specific and prescriptive security requirements for information security programs, similar to the cybersecurity regulations issued by the New York Department of Financial Services (NYCRR 500). For example, the proposed amendments would require that financial institutions protect by encryption all customer information held or transmitted, both in transit over external networks and at rest. Furthermore, the new rules would require financial institutions to implement multi-factor authentication (MFA) for any individual accessing customer information. The MFA would need to include at least two of the three following factors: (1) Knowledge Factor (e.g., passwords, biographical information); (2) Possession Factor (e.g., tokens, possession of devices); and (3) Inherence Factor (e.g., biometric characteristics such as fingerprints or voice). The rules would allow for financial institutions to implement alternative controls if they are approved by the Chief Information Security Officer (CISO).

Provisions Designed to Improve Accountability. The NPRM also proposes adding provisions designed to improve the accountability of a financial institution's information security program. For example, the revised rule would require financial institutions to designate a single qualified individual CISO, who is responsible for overseeing, implementing, and enforcing the information security program. The CISO would also be required to provide an annual written report to the Board of Directors or equivalent governing body regarding the status of the information security program. The amendments would also require institutions to base their security programs on a written risk assessment and require institutions to periodically perform additional risk assessments and regulatory tests, or to otherwise monitor the effectiveness of the program.

Exemption for Small Business From Certain Requirements. The proposed amendments would exempt smaller financial institutions that maintain relatively small amounts of customer information (those that maintain customer information concerning fewer than 5,000 customers) from the requirements for written assessments. Businesses qualifying for the exemption would not be required to generate a written risk assessment, a continuous monitoring or annual penetration testing and biannual vulnerability assessment, a written incident response plan, or the annual written report required of the CISO.

Expansion of the Scope of Covered "Financial Institution." The proposed amendments would expand the scope of a covered "financial institution" to explicitly include "finders," who charge a fee to connect consumers who are looking for a loan to a lender. The definition of a covered financial institution under the GLBA is not precise and the agency has at times used enforcement actions, rather than rulemaking, to map out the scope of coverage – for example, by bringing a recent GLBA enforcement action against a third-party software provider dealing with financial data used in credit transactions. The amendments would further include the definition of "financial institution" and related examples in the Rule itself rather

than cross-reference them from a related FTC rule, the Privacy of Consumer Financial Information Rule.

The Workshop Explored Practical Application of the Proposed Rules, As Well As Costs and Benefits. The workshop began with opening remarks from FTC staff attorney David Lincicum, who outlined the main requirements of the current Safeguards Rules, as well as the proposed amendments. Lincicum explained that the goal of the workshop was to engage with stakeholders with direct experience providing information security and better understand the costs and benefits of the practices set forth in the proposed rule (particularly for smaller businesses).

The FTC held five panel discussions with experts in industry, academia, and government on the following topics:

- Panel 1: The Costs and Benefits of Information Security Programs
- Panel 2: Information Security Programs and Smaller Businesses
- Panel 3: Continuous Monitoring, Penetration, and Vulnerability Testing
- Panel 4: Accountability, Risk Management, and Governance of Information Security Programs
- Panel 5: Encryption and Multifactor Authentication

Common themes that panelists discussed throughout the day included the importance of outcome-driven rules; the need for a framework that contemplates increased use of cloud vendors; the high costs of maintaining a comprehensive information security program; and the impact of the rules on internal processes such as documentation, among others.

The workshop was initially scheduled to take place on May 13, 2020, but was rescheduled due to coronavirus-related (COVID-19) disruptions. The FTC is accepting comments through **August 12, 2020**.

If you have questions about the workshop or are interested in filing comments, please contact the one of the authors listed on this alert.

---

1 *See* 16 C.F.R § 314.3.

2 *See* Public Law 106-102, 113 Stat. 1338 (1999).