wiley

ALERT

FTC Announces Proposed Changes to Cybersecurity Regulation for Financial Institutions

March 6, 2019

On Tuesday, March 5, the Federal Trade Commission (FTC) announced proposed revisions to its Safeguards Rule, which governs data security practices for financial institutions under the FTC's Gramm-Leach-Bliley (GLB) Act jurisdiction. The proposed revisions—which were issued by a 3-2 vote—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. This proposal marks a distinct shift in the FTC's approach to data security for financial institutions. The proposed revisions opt for a top-down, regulatory approach akin to New York's Department of Financial Services (DFS)'s cybersecurity regulation, which also mandates certain data security practices, including encryption and multi-factor authentication. As the two dissenting Republican Commissioners describe it, "[t]he current proposal . . . trades flexibility for a more prescriptive approach."

The FTC's Safeguards Rule requires covered financial institutions to develop, implement, and maintain a comprehensive information security program containing safeguards to collect and handle customer information. The safeguards must be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated security threats, and protect against unauthorized access or use that could result in substantial harm or inconvenience. The safeguards must be appropriate to the size and complexity of the company, the nature and scope of its activities, and the sensitivity of the customer data.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

FTC and Consumer Protection

Privacy, Cyber & Data Governance

The proposed amendments, in the Commission's view, "continue to provide companies with flexibility, [but] also attempt to provide more detailed guidance as to what an appropriate information security program entails."[1] And the Commission cited, with approval, previous industry comments suggesting that non-bank financial technology companies—fintechs—should be subject to rules akin to those applicable to banks under Federal Financial Institutions Examination Council (FFIEC) Interagency Guidelines. The proposed requirements include:

- Developing a cybersecurity incident response plan;
- Designating a single individual to coordinate the company's information security program;
- Basing the information security program on a risk assessment and periodically performing additional risk assessments;
- Placing access control on information systems to authenticate users and permit access only to authorized individuals;
- Identifying and managing data, personnel, devices, systems, and facilities;
- Restricting access to physical locations containing customer information only to authorized individuals;
- Encrypting all customer information, both in transit and at rest;
- Adopting secure development practices for in-house developed applications for transmitting, accessing, or storing customer information;
- Implementing multi-factor authentication for any individual accessing customer information or internal networks that contain customer information;
- Including audit trails designed to detect and respond to security events;
- Developing procedures for the secure disposal of customer information no longer necessary for business operations or other legitimate business purposes;
- Adopting procedures for change management, which govern the addition, removal, or modification of elements of an information system;
- Implementing policy and procedures to monitor the activities of unauthorized users and detect unauthorized access to customer information;
- Implementing training and education policies to enact the information security program;
- Monitoring service providers to assess the adequacy of their safeguards on an ongoing basis;
- Requiring the chief information security officer to provide certain annual reports about information security to the company's Board of Directors

In the Notice of Proposed Rulemaking (NPRM), the FTC also seeks comment on whether financial institutions should be required to report security events to the Commission, and whether a Board should be required to certify compliance with the Rule. It also proposes to exempt institutions with relatively small amounts of customer information from certain parts of the Rule.

Additionally, the proposed amendments would expand the scope of "financial institutions" covered under the rule to include companies significantly engaging in activities "incidental to financial activities." And in particular, the definition would include companies acting as "finders"– with "finding" defined as bringing together buyers and sellers of products or services for transactions that the buyers and sellers themselves negotiate and consummate. The Commission suggested that these companies should be subject to safeguard requirements because "they collect, maintain, and store sensitive consumer information . . . [and] [i]f this sensitive information were to get into the wrong hands, consumers could suffer identity theft, fraud, or other harms."[2]

Notably, Commissioners Noah Phillips and Christine Wilson dissented from the NPRM, arguing that the proposed regulations may not be appropriate for all market participants, are premature to enact, and conflict with the existing flexible approach to data security—imposing costs without clear consumer benefits. They also criticize the proposals for substituting the Commission's own judgment for private companies' governance decisions.

Additionally, in a separate NPRM, the Commission is seeking comment on proposed revisions to its Privacy Rule under the GLB Act. Unlike the vote on the Safeguards Rule NPRM, the vote on the Privacy Rule proposal was 5-0.

For both NPRMs, comments will be due in 60 days after publication in the Federal Register.

---

[1] Notice of Proposed Rulemaking ("NPRM") at 5.

[2] NPRM at 19.