The Investment Lawyer
Covering Legal and Regulatory Issues of Asset Management
VOL. 29, NO. 2 • FEBRUARY 2022

REGULATORY MONITOR

FTC Update

By Daniel K. Alvarez, Laura E. Jehl, Richard M. Borden, Kari Prochaska, and Amelia Putnam

FTC Establishes New Cybersecurity Benchmarks

Last October, the Federal Trade Commission (FTC) amended its Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (Rule) to, among other things, modify the scope of companies to which the Rule applies and impose new, detailed and enforceable requirements as to the information security programs and practices those companies must adopt. The FTC's Safeguards Rule applies directly to any financial institutions that fall under the FTC's GLBA jurisdiction, and those companies must now evaluate whether their existing security controls and practices comply with the new Rule and implement any necessary new measures or take appropriate steps to come into compliance. More broadly, however, the amendments (1) reflect the Biden Administration's strategy to push companies to improve their cyber hygiene, and (2) create new benchmarks for data security that the FTC seems likely to incorporate into other data protection enforcement and rulemaking activities and that may find their way into judicial interpretations of consumer protection and similar statutes in the context of proper handling of consumer data. As a result, even companies outside the financial industry may need to reconsider their data protection practices in the wake of these amendments.

Modified Scope

The GLBA regulates the privacy and data security practices of "financial institutions," defined to include not only banks but also mortgage brokers, payday lenders, real estate appraisers and non-bank lenders. The amended Rule modifies the scope of covered financial institutions in two ways:

1. It includes "finders" as covered financial institutions, and defines this new concept as entities that "bring[] together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate;" and
2. It exempts smaller financial institutions that maintain customer information for fewer than 5,000 individuals from having to comply with some provisions of the Rule.

Companies that may not have been subject to GLBA before will need to consider whether they are "finders" under the new definition.

New Information Security Requirements

The amended Rule sets forth specific criteria for financial institutions' information security programs, as well as other data protection requirements, that are new to the FTC's Safeguards Rule, though as

discussed below some of these requirements may not be new to companies that have had to comply with certain state-level requirements. Examples of these requirements include:

- Designating a qualified individual to oversee and enforce the information security programs, and having that individual provide status reports to the board of directors or similar governing body;
- Conducting a risk assessment that identifies reasonably foreseeable risks to the security of customer information, as well as the sufficiency of existing controls and the risk of unauthorized use or disclosure of customer information, builds the information security program on that foundation, and revises the program based on regular risk assessments conducted moving forward;
- Conducting regular testing and monitoring of key security controls, systems, and procedures;
- Implementing specific tools for data protection, such as multi-factor authentication for accessing any information system, and encryption for customer information in transit over external networks and at rest, subject to certain exceptions;
- Crafting a written incident response plan that is designed to permit prompt response to and recovery from any material security event;
- Periodically reviewing access controls to authenticate and allow access only to authorized individuals and limit those individuals' access to information;
- Developing and maintaining data retention procedures that provide for the secure disposal of customer information *within two years*, unless the information is necessary for a legitimate business purpose or otherwise unfeasible; and
- Implementing controls to monitor the log activity of authorized users in order to detect unauthorized access or use.

Key Similarities and Differences with the New York Department of Financial Services Cybersecurity Regulation

As mentioned, many of these requirements are similar or identical to certain state data protection requirements, including those imposed on financial institutions doing business in New York by the New York Department of Financial Services (NYDFS) Cybersecurity Regulation.[1] For example, both the amended Safeguards Rule and the NYDFS Cybersecurity Regulation require financial institutions to, among other things: (1) conduct a cybersecurity risk assessment; (2) evaluate existing information security controls; (3) implement additional risk-based controls; (4) limit access to information systems and customer information for a necessary business purpose; and (5) utilize multifactor authentication.

While the FTC may look to DFS's interpretations and enforcement of the Cybersecurity Regulation for lessons learned, there are also important differences between the Safeguards Rule and Cybersecurity Regulation that financial institutions should track. For example, the amended Safeguards Rule requires entities to periodically dispose of customer information no later than two years after the last date the information was used for a business purpose, whereas the Cybersecurity Regulation requires periodic disposal, but does not prescribe timing.

Moving Forward

The right next steps for your company likely depend on which of three buckets applies to you:

1. Companies that have always been subject to the FTC's Safeguards Rule need to consider whether their existing practices measure up to the new requirements, and take action to shore up areas where their practices may fall short;
2. Companies that may find themselves newly subject to the rule as a result of the expanded scope may need to consider whether the business

activities that bring them in-scope are worth the compliance cost and risk and, if so, take steps to bring themselves into compliance; and

3. Companies that are subject to the FTC's general jurisdiction should continue to monitor developments and even consider ways to incorporate these practices into their existing programs, because the FTC has a history of using sector-specific rule-makings as a way to establish new benchmarks that it will subsequently use in broader enforcement and policy-making activities. Likewise, companies that may find themselves subject to enforcement under consumer protection and similar laws should monitor the extent to which courts look to these and analogous requirements as benchmarks for what may be generally expected of companies handling consumer data.

Mr. Alvarez and **Ms. Jehl** are partners and Co-Chairs of the Cybersecurity & Privacy Practice Group at Willkie Farr & Gallagher LLP in Washington, DC. **Mr. Borden** is counsel at Willkie Farr & Gallagher LLP in New York, NY. **Ms. Prochaska** is an associate at Willkie Farr & Gallagher LLP in Chicago, IL. **Ms. Putnam** is an associate at Willkie Farr & Gallagher LLP in Washington, DC.

NOTE

[1] 23 NYCRR 500, the "Cybersecurity Regulation."