Raising the Bar: FTC's Proposed Changes to the Safeguards Rule Would Establish a New Standard for Information Security Programs

Alyssa Z. Hutnik

March 7, 2019

The Federal Trade Commission (FTC) announced this week that it is seeking comments on proposed amendments to the Privacy Rule and Safeguards Rule under the Gramm-Leach-Bliley Act (GLBA). These two rules outline obligations for financial institutions to protect the privacy and security of customer data in their control. While the proposed changes to the Privacy Rule are modest, the expansive list of specific cyber controls proposed for the Safeguards Rule is material and could impose a new de facto minimum security standard that implicates many businesses, including those outside the coverage of the Rule.

Privacy Rule

The Privacy Rule, which went into effect in 2000, requires a financial institution to inform customers about its information-sharing practices and allow customers to opt out of having their information shared with certain third parties. Changes to the Dodd-Frank Act in 2010 transferred the majority of the FTC's rulemaking authority for the Privacy Rule to the Consumer Financial Protection Bureau. Only certain motor vehicle dealers are still subject to FTC rulemaking under the Privacy Rule. To address these changes, the proposed amendments would remove from the Rule examples of financial institutions that are no longer subject to FTC rulemaking authority, and provide clarification to motor vehicle dealers regarding the annual privacy notices.

Safeguards Rule

The Safeguards Rule, which went into effect in 2003, requires financial institutions to develop, implement, and maintain comprehensive information security programs to protect their customers' personal information. Currently, the Safeguards Rule emphasizes a process-based approach that is flexible in how the program is implemented so long as it meaningfully addresses core components, and where the safeguards address foreseeable internal and external cyber risks to customer information.

The proposed amendments to the Safeguards Rule would still follow a process-based approach but add significantly more specific requirements that must be addressed as part of the company's information security program. These include, for example:

- Appointing a Chief Information Security Officer (CISO) (e.g., a qualified individual responsible for

overseeing and implementing the information security program and enforcing the program). The CISO can be an employee, affiliate, or a service provider, but if the latter, additional requirements apply;

- More specificity in what the required information security program's risk assessments involve;
- More specificity in what is required as part of a company's access controls for their information systems;
- Updating risk assessments and resulting safeguards concerning a company's data and system identification and mapping;
- Employing encryption of all customer information stored or transmitted over external networks or implement alternative compensating controls that are reviewed and approved by the company's CISO;
- Adopting secure development practices for in-house developed applications that handle customer information;
- Implementing multi-factor authentication for any individual with access to customer information or internal networks that contain customer information (unless the CISO approves a compensating control);
- Including audit trails that detect and respond to security events;
- Implementing change management procedures;
- Implementing safeguards that both monitor authorized activity and detect unauthorized activity involving customer information;
- Regular testing of the effectiveness of the information security program's key controls, systems, and procedures, including continuous monitoring or annual penetration testing and biannual vulnerability assessments;
- Establishing a written incident response plan that addresses goals, outlines the internal processes for incident response, defines clear roles, responsibilities and levels of decision-making authority, identifies external and internal communications and information sharing, identifies requirements for the remediation of identified weaknesses in information systems and controls, addresses the documentation and reporting of security events and related incident response activities, and the evaluation and revision of the program, as needed post-incident;
- Requiring the CISO to at least annually report to the board of directors or equivalent governing body on the status of the information security program, the company's compliance with the Safeguards Rule, and material matters related to the information security program.

The proposed modifications would exempt small businesses (financial institutions that maintain customer information concerning fewer than five thousand consumers) from some of the Safeguard Rule's requirements.

In addition, the proposed modifications would expand the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities (e.g., "finders" that bring together buyers and sellers of a product or service), and incorporate the definition of this term directly in the Safeguards Rule, instead of by reference based

on the Privacy Rule.

Two Republican appointed-Commissioners, Noah Phillips and Christine Wilson, dissented from the proposed amendments, noting that it may not be appropriate to mandate such prescriptive standards for all market participants. They maintained that producing guidance for companies would be a better approach than one-size-fits-all amendments that all companies will have to follow. The Commissioners also made a case that the proposed amendments are based on the New York State Department of Financial Services cyber regulations, which are too new for the FTC to evaluate for impact or efficacy. They also expressed concerns with the rigidity that these new requirements would place on what is now a flexible approach, and whether these amendments would place the Commission in the stead of a company's governance in deciding the level of board engagement, hiring and training, and accountability design, among other controls.

***

While the proposed amendments are limited to financial institutions subject to the GLBA Privacy Rule and Safeguards Rule, if adopted, the specificity of the cyber controls proposed are likely to factor into contract terms that financial institutions impose on their partners and service providers, as well as serve as a potential model for other industries. If adopted, these would be the most explicit cyber regulations in the United States to date. At the same time, it is notable that the agency declined to adopt a safe harbor based on a showing of compliance with an industry standard, such as NIST or PCI DSS. In other words, the proposed changes suggest a potential new minimum standard for enterprise security programs that warrant close consideration. Given the influential role that the Safeguards Rule played in developing information security programs outside of the financial sector, these new proposed requirements may well become the de facto industry standard if history is a guide.

The deadline to submit written comments will be 60 days after the notice is published in the Federal Register. We will continue to monitor these developments.