Published on *The National Law Review* https://natlawreview.com

FTC Finalizes Updated Safeguards Rule Under GLBA to Dramatically Expand Data Security Requirements and Scope of Rule

Article By:

Benjamin William Perry

Courtney M. Achee

Until now, companies primarily regulated by the Federal Trade Commission (FTC) were given only vague directives to implement systems sufficient to safeguard customer data, coupled with FTC "recommendations" as to best practices. That is about to change with the FTC's finalization of its proposed amendments to the Standards for Safeguarding Customer Information (Safeguards Rule) on October 27. The new requirements will become effective one year after the rule is published in the Federal Register, so companies should start planning for compliance now to avoid fire drills down the road.

The new Safeguards Rule is more aligned with the requirements imposed by the Federal Financial Institutions Examination Council (FFIEC) for banking and depository institutions and, in some respects, imposes more burdensome requirements. Companies subject to the FTC's authority should start prepping now to ensure that their current data security practices and infrastructure — and those of their service providers — will survive FTC scrutiny.

Who Is Covered by the Amended Safeguards Rule?

The FTC's jurisdiction applies to a surprisingly broad range of businesses. This updated rule applies to entities traditionally within the FTC's jurisdiction for rulemaking and enforcement, which include non-banking (non-depository) institutions such as mortgage brokers, mortgage servicers, payday lenders, and other similar entities.

But the FTC's jurisdiction does not end there, and in fact, the rule's definition now encompasses companies that never traditionally would be considered "financial institutions." For example, the scope of the new rule now broadly applies to businesses that bring together buyers and sellers of a product or service, potentially drawing in companies of all shapes and sizes, such as marketing companies. Furthermore, the FTC has previously determined that higher education institutions also fall within the definition of "financial institutions," and thus are subject to the rule's requirements, because higher education institutions participate in financial activities, such as making federal student

loans.

Businesses operating in any of these industries should take note of these important changes and determine whether sweeping changes to existing information security programs are necessary.

What Are the Biggest Takeaways?

There are a number of changes contained in the final Safeguards Rule, but the biggest takeaways are:

1. The definition of “financial institution” has been dramatically expanded to include “finders,” or entities that bring together buyers and sellers of any product or service for transactions;

2. More specific requirements for information security programs were imposed, including encryption for data both in transit and at rest;

3. A new small business exception to the Safeguards Rule’s requirements was added;

4. Mandatory requirements for risk assessments (which now must be set forth in writing) were established; and

5. Required periodic reporting on information security programs to boards of directors or governing bodies was implemented.

We will explore some of these noteworthy changes in greater detail.

Expanded Definition of “Financial Institution”

The definition of “financial institution” has now been expanded to include a “finder,” which is defined as a company that “bring[s] together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate.” To support this change, the FTC reasoned that finders often possess sensitive consumer financial information and should be subject to the requirements of the Safeguards Rule in protecting it from unauthorized disclosure.

Commenters on the proposed rule expressed grave concerns that the term “finder” is overly broad and would inappropriately sweep large swaths of companies into the definition of a “financial institution.” The Association of National Advertisers also expressed concern that advertisers could constitute “finders” under this definition due to their role in connecting buyers and sellers. However, the FTC noted that the although the definition is broad, its scope is significantly limited because the Safeguards Rule applies only to the information of customers and “it will not apply to finders that have only isolated interactions with consumers and that do not receive information from other financial institutions about those institutions’ customers.” It remains to be seen how broadly the term “finder” will be construed, and this could prove to be one of the biggest question marks of the scope of the new rule.

Specific Data Protection Requirements

Whereas the FTC previously left specific aspects of satisfactory information security systems up to

the discretion of the business, the FTC now requires that financial institutions address the following:

- Access controls;
- Data inventory and classification;
- Encryption;
- Secure development practices;
- Authentication;
- Information disposal procedures;
- Change management;
- Testing; and
- Incident response.

The biggest takeaway here is that the FTC is imposing more specific requirements, such as encryption, for the protection of sensitive customer information, whereas the previous Safeguards Rule allowed financial institutions to exercise discretion by referring to data protection in generalities. In addition, the rule's encryption requirements, which include encrypting data both in transit and at rest, are more burdensome than the FFIEC's proposed guidelines, which do not require banks to encrypt data at rest unless the institution's risk assessment determines that such encryption is necessary.

Mandatory Periodic Reporting

The new rule now requires that a financial institution's chief information security officer must now report in writing, at least annually, to the financial institution's board of directors or governing body regarding the following:

- The overall status of the information security program and financial institution's compliance with the Safeguards Rule; and
- Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

If the company does not have a board of directors or equivalent governing body, the chief information security officer must "make the report to a senior officer responsible for the financial institution's information security program."

Small Business Exemption

The new rule adds a “small business” exemption, which excludes businesses that “maintain customer information concerning” fewer than 5,000 consumers from the following requirements of the new rule:

- Requiring a written risk assessment (314.4(b)(1));
- Requiring continuous monitoring or annual penetration testing and biannual vulnerability assessment (314.4(d)(2));
- Requiring a written incident response plan (314.4(h)); and
- Requiring an annual written report by the chief information security officer (314.4(i)).

It remains to be seen, however, how many businesses will be able to take advantage of this exception as a practical matter, especially for businesses that are required to maintain consumer records for a certain number of years.

Other Noteworthy Changes

In addition to the important changes outlined above, there are also several other important changes to note. Although not intended to be exhaustive, the list of other changes include:

- The addition of a definition for “authorized user,” which means “any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.” This term was added in conjunction with specific data access restriction requirements and more specific requirements for monitoring anomalous patterns of usage by “authorized users.”
- The definition of “security event” now includes the compromise of customer information in physical form, as opposed to only electronic form.
- The new rule imposes mandatory requirements for risk assessments (which now must be set forth in writing). Risk assessments were already required, but requirements are now more explicit.

Takeaways

In light of these updates, financial institutions should review their policies and procedures, as well as their contracts with service providers, to ensure that all security information systems comply with the new, detailed security requirements of the amended Safeguards Rule. As always, an ounce of prevention on the front end will highly reduce the risk of an FTC enforcement action or consumer litigation down the line.

National Law Review, Volumess XI, Number 306

Source URL:https://natlawreview.com/article/ftc-finalizes-updated-safeguards-rule-under-glba-to-dramatically-expand-data