



November 7, 2016

Via electronic submission to <https://ftcpublishcommentworks.com/ftc/safeguardsrulenprm>

Donald S. Clark
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Safeguards Rule, 16 CFR 314, Matter No. P145407

Dear Mr. Clark,

The Financial Services Roundtable/BITS¹ (“FSR/BITS”) appreciates this opportunity to provide comments regarding the Federal Trade Commission’s (“FTC,” or “Commission”) Standards for Safeguarding Customer Information (“Safeguards Rule” or “Rule”), as part of the FTC’s systematic review of all current Commission regulations and guides.

We focus our comments on three areas: (1) the importance of maintaining the provisions of the Safeguards Rule as is; (2) the importance of harmonizing the Safeguards Rule with the NIST Cybersecurity Framework; and (3) the need to preserve the scope of the term “financial institution” as currently espoused in the Rule.

I. Financial Services Sector Leadership on Cybersecurity Practices and Regulation

The financial services industry, as a sector, is a leader in cybersecurity. Since the advent of the Internet and the migration of financial services to the online sphere, the financial services sector has demonstrated a robust and sustained commitment to ensuring the protection of customer information and the integrity of financial systems and networks. The best-in-class security protocols and controls developed by the financial services sector are the product of intense study and dedicated research devoted to the pursuit of innovation and the deployment of new security technologies to protect financial information. These advancements driven by

¹ About FSR and BITS: As advocates for a strong financial future™, FSR represents the largest integrated financial services companies providing banking, insurance, payment and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America’s economic engine, accounting directly for \$92.7 trillion in managed assets, \$1.2 trillion in revenue, and 2.3 million jobs. BITS is the technology policy division of FSR and addresses newly emerging threats and opportunities, particularly those related to cybersecurity, fraud reduction and critical infrastructure protection. Working with CEOs, CIOs, heads of IT Risk and other senior members of member companies, BITS identifies key issues at the intersection of financial services, technology and commerce and facilitates collaboration to improve the ecommerce environment for member companies and their customers through the development of policies and practices.



collective investment by the sector will continue, and will extend into in the areas of mobile devices, cloud services, and beyond.

In part, the sector’s leading security practices and processes reflect the sensitivity of the data itself and the consequences that would arise for consumers and the economy as a whole should financial services networks and system be compromised significantly or repeatedly.

The industry also was the first to formalize information sharing about threats and vulnerabilities, through the establishment of the information sharing and analysis center FS-ISAC. FS-ISAC is recognized globally as the gold standard for industry collaboration and for its dedication to the mission of reducing cybersecurity risks through the process of individual companies sharing information related to attempted and successful cyberattacks, so that the entire industry can benefit from the knowledge and experience.

Throughout this time, financial institutions have been subject to rigorous and comprehensive cybersecurity regulations, supervisory guidance and are regularly examined by federal and state authorities. These include the Gramm-Leach-Bliley Act of 1999 (including the “Interagency Guidelines Establishing Information Security Standards” regulation), the Fair Credit Reporting Act, the Right to Financial Privacy Act as well as extensive regulations, and supervisory guidance from the Federal Financial Institutions Examination Council addressing information security, vendor management and business continuity risks.

Subsequently, in February 2013, President Obama directed the Department of Commerce, through NIST, to develop a voluntary framework for improving critical infrastructure cybersecurity.² From the start, the financial services sector was supportive and engaged in this process, participating in all six NIST cybersecurity workshops and submitting responses to the various Federal Register requests for information.

FSR/BITS played a key role in coordinating the financial sector’s input through the Financial Services Sector Coordinating Council (FSSCC), serving as the policy co-chair on the FSSCC during the comment period after the Preliminary Framework was released. FSR/BITS also gathered policy makers, thought leaders, and representatives from member companies at additional events and submitted two substantive comment letters.³ The final “Framework for Improving Critical Infrastructure Cybersecurity,” released by NIST (NIST Framework) includes several of the recommendations provided by the financial services sector, including the decision to adopt a risk-based methodology.

The open and transparent process that led to the NIST Framework resulted in a document that has been widely embraced beyond the critical infrastructure sector by thousands of businesses and enterprises and across all sectors of the economy. As a tool for helping organizations adopt a cybersecurity risk management program, the NIST Framework operates as

² Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 12, 2013).

³ See, e.g., http://csrc.nist.gov/cyberframework/rfi_comments/040813_fsscc.pdf.



a type of “Rosetta Stone” that translates sector specific cybersecurity language into a common lexicon to be used across sectors.

The following comments reflect the FSR membership’s collective perspective as leaders in the development and implementation of best-in-industry cybersecurity practices as well as active participants in the advancement of cybersecurity regulatory constructs.

II. Maintaining the Provisions of the Safeguards Rule

As stated in the Federal Register notice, the FTC is seeking comment on whether there is a “continuing need for specific provisions of the Rule?”⁴ In response to this question, we submit that all provisions of the Safeguards Rule should be maintained. The information security requirements imposed by the Safeguards Rule have been held by several agencies, including the FTC, as a model set of elements comprising an information security program. These elements should remain intact for purposes of providing continued, comprehensive direction on the development and adequacy of information security programs in the financial services sector.

III. Harmonization of the FTC Safeguards Rule with the NIST Cybersecurity Framework

The FTC is also seeking comment on whether the Rule “[s]hould...be modified to reference or incorporate any other information security standards or frameworks, such as the National Institute of Standards and Technology’s Cybersecurity Framework...”⁵ In response to this question, we believe that the FTC Safeguards Rule would benefit from reference to the NIST Framework. Specifically, we recommend that the Rule be modified to reference and leverage the NIST Framework as a means of establishing compliance with the Safeguards Rule. In other words, per the proposed modification, financial institutions that use the NIST Framework to develop an information security program would be found in *de facto* compliance with the Rule. To facilitate the inclusion of the Framework as an approach under the Safeguards Rule, we further recommend the creation of a guidance document mapping the safeguards requirements against the NIST Framework and the newly released, higher-level G-7 “Fundamental Elements of Cybersecurity for the Financial Sector.”⁶

As discussed above, the NIST Framework represents an important achievement in the advancement of cybersecurity risk management across all parts of government and the economy. When the FTC issued the original Safeguards Rule in 2002, such a framework did not exist and the issue of cybersecurity was not at the forefront of the policymaking agenda or American businesses priorities. In this sense, we think it is particularly important that the FTC’s efforts with respect to the Safeguards Rule complement and reference the NIST Framework, which in

⁴ 81 Fed. Reg. 61,634.

⁵ 81 Fed. Reg. 61,635.

⁶ See <https://www.treasury.gov/press-center/press-releases/Pages/jl0570.aspx>; see also <https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf>.



turn was informed by existing cybersecurity standards adopted by the U.S. financial services industry.

Harmonizing the Safeguards Rule with the NIST Framework by using the Framework as an informative reference would advance the objectives of the Rule by adopting a more modern and flexible standard designed for today's cybersecurity challenges and optimized to confront those challenges in the most efficient and effective way. The effort would actualize the statutory directive to provide for administrative, technical, and physical safeguards for customer information.⁷

At the same time, doing so would move a step in the right direction of starting to address the growing thicket of cybersecurity compliance obligations that are spreading across the financial services sector, which is subject to a significant number of federal and state laws, regulations, guidance, and examination standards relating to cybersecurity. Many of these laws and policies emanate from the general financial safety and soundness standards and customer information security provisions contained within the Gramm-Leach-Bliley Act of 1999.

The most significant development since the FTC last reviewed its Safeguards Rule has been that cybersecurity has achieved status as a prominent, even paramount, issue for many financial regulators, and many of those regulators are engaged in ongoing efforts to address cybersecurity issues faced by the entities that they regulate. As is often the case with regulatory efforts that are new and evolving, different financial regulators are still trying to make sense of the regulatory landscape, and are using different types of regulatory tools, moving at different speeds, and using differing taxonomies and degrees of comprehensiveness.

For example, within the past two months alone, the New York Department of Financial Services,⁸ the Federal Reserve Board in tandem with the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation,⁹ and the Financial Crimes Enforcement Network¹⁰ each issued cybersecurity regulatory proposals or related guidance. Within the past year, the Federal Financial Institutions Examination Council's ("FFIEC," or "Council") issued a new Cybersecurity Assessment Tool as part of the prudential regulation regime of the banking regulators and their holding companies, and has begun to incorporate it into its examination processes.¹¹ The Commodity Futures Trading Commission ("CFTC") has finalized rules that would apply certain cybersecurity standards to derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data

⁷ 15 U.S.C. §§ 6801(b), 6805(b)(2).

⁸ See <http://www.dfs.ny.gov/about/press/pr1609131.htm>.

⁹ 81 Fed. Reg. 74,315

¹⁰ See https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

¹¹ See <https://www.ffiec.gov/cyberassessmenttool.htm>.



repositories.¹² The Securities and Exchange Commission (“SEC”) has been engaged in issuing more piecemeal cybersecurity guidance, primarily through subdivisions of the agency like the Office of Compliance Inspections and Examinations (“OCIE”) and the Division of Investment Management. The Financial Industry Regulatory Authority (“FINRA”) and National Futures Association (“NFA”), the self-regulatory organizations (“SROs”) that enforce many of the nation’s securities, commodities, and derivatives trading laws, also have been active on cybersecurity regulation. In early 2015, FINRA issued a report intended to help broker-dealers and others address cybersecurity issues, and in October 2015, the NFA issued a new interpretive notice regarding protection of Information Technology (“IT”) systems containing customer or financial information.

In addition to being at times contradictory and superfluous, these various and substantial compliance obligations are imposing significant resource costs on businesses and are affecting the ability of enterprises to institute customized information programs that reflect their unique needs, instead creating compliance-focused programs that depart from entities’ optimal cybersecurity posture. In the two years since it was issued, the Framework has been widely followed among financial firms, yet inconsistencies between the Framework and the emerging regulatory guidance noted above is diverting a scarce resource – cybersecurity professionals – from security related activities toward more question-and-answer “translation and mapping” exercises. Incorporating the NIST Framework as an informative reference under the Safeguards Rule will serve as a key initial step in harmonizing regulatory efforts and moving us in the direction of a more cohesive approach to addressing cybersecurity concerns. Indeed, if further regulatory agency particularization occurs, the ability for firms to achieve a common cyber understanding across sectors will be substantially impeded, yielding a more negative security outcome for the nation, the sectors, firms, and thus, citizens and consumers.

III. Use of term “financial institution”

The Safeguards Rule applies to all “financial institutions” over which the Commission has jurisdiction. The Safeguards Rule uses the definition of “financial institution” from the Privacy Rule. The Privacy Rule defines “financial institution” as “any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution significantly engaged in financial activities is a financial institution.”

The term “financial activities” includes not only a number of traditional financial activities specified in 12 U.S.C. 1843(k), but also those activities found by the Federal Reserve Board (“the Fed”) to be closely related to banking by regulation “in effect on the date of the enactment” of the GLBA.

The current Safeguards Rule incorporates the Privacy Rule’s definition of “financial institutions” as entities that are significantly engaged in financial activities, including activities

¹² See <http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816c.pdf>; <http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/federalregister090816b.pdf>.



found to be closely related to banking by regulation or order in effect at the time of enactment of GLBA.

The Commission asked several specific questions about the role of the definition of “financial institution” in the Safeguards Rule, below we address several of these questions.

- a. *Should the Safeguards Rule’s definition of “financial institution” be modified to also include entities that are significantly engaged in activities that the Federal Reserve Board has found to be incidental to financial activities?*

No, FSR/BITS suggests that the current definition referenced in the Safeguard Rule is sufficient to address the FTC’s authorities. The Rule should not be modified to include activities incidental to financial activities. This could serve as a dramatic expansion of the Rule’s reach, which could have the effect of adding to regulatory confusion and overlap and stifling innovation through imposing unnecessary compliance standards on activities and business models that are already regulated by prudential and state regulators.

- b. *Should it also include activities that have been found to be closely related to banking or incidental to financial activities by regulation or order in effect after the enactment of GLBA?*
- c. *If so, should all such activities be included in the modified definition? What evidence supports such a modification?*

FSR/BITS has not seen evidence that would lead us to believe that some of these activities are not covered by current regulation by financial institutions themselves. As the FTC looks into financial activities beyond the scope of financial institutions, we urge you to work closely with the FFIEC to ensure that you are limiting duplication, overlap and possible confusion for all of those regulated under GLBA.

* * *

Thank you for considering our views. If you have any questions or would like to discuss further, please contact us, or our colleague, Josh Magri at Josh.Magri@FSRoundtable.org.

Sincerely,

Richard Foster
Senior Vice President & Senior Counsel for
Regulatory and Legal Affairs
Financial Services Roundtable

Christopher F. Feeney
President
BITS | Financial Services Roundtable
Chris.Feeney@FSRoundtable.org



Richard.Foster@FSRoundtable.org