



**SIIA**

Accelerating Innovation in  
Technology, Data & Media

202.289.7442  
[www.siiia.net](http://www.siiia.net)

1090 Vermont Ave NW Sixth Floor  
Washington DC 20005-4905

November 7, 2016

Donald S. Clark  
Secretary  
Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Avenue NW  
Washington, DC 20580

Dear Mr. Clark,

On behalf of the Software & Information Industry Association (SIIA), thank you for the opportunity to comment on the Federal Trade Commission (“FTC” or “Commission”) review of the Standards for Safeguarding Customer Information (“Safeguards Rule” or “Rule”).

SIIA is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society, including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength—software alone contributes \$425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs.<sup>1</sup>

While most SIIA member companies are not financial institutions, many large and small companies provide technical services or receive customer information from financial institutions. On behalf of our members and the industry, please find below three recommendations as you review and consider modifications to the Safeguards Rule.

### **1. The Safeguards Rule Should Remain Flexible, Particularly to Enable Compliance by Small, Innovative Companies**

It has been 14 years since the Gramm-Leach-Bliley Act (GLBA) created the requirement for the FTC to establish Standards for Safeguarding Customer Information (“Safeguards Rule” or “Rule”). Implementation of this Rule took place in 2003, when internet-based

---

<sup>1</sup> The U.S. Software Industry: An Engine for Economic Growth and Employment; SIIA; 2014, <http://www.siiia.net/Admin/FileManagement.aspx/LinkClick.aspx?fileticket=ffCbUo5PyEM%3d&portalid=0> .

financial services were growing rapidly, but methods for safeguarding sensitive data were still evolving. Fortunately, like many internet policies of that time, the Safeguards Rule recognized the need for a clear principles-based approach, and a light regulatory touch. In crafting the initial Rule, the Commission was right to emphasize flexibility, rather than creating a prescriptive set of one-size-fits-all security requirements.

The Safeguards Rule was intended to be flexible to accommodate the wide range of entities covered by GLBA, as well as the wide range of circumstances many additional companies face in securing customer information. Accordingly, the Rule requires financial institutions to implement a written information security program that is appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

This is the right approach, as it recognizes a wide range of threats faced by a diverse set of businesses, with varying levels of sophistication and capabilities for addressing these threats. The flexible approach created by the Safeguards Rule is necessary to account for these critical differences, rather than seeking to establish specific security requirements that are likely to become obsolete, outdated or conflicting with other requirements layered at the federal or state level. Ultimately, a more prescriptive regulatory approach for the Rule would not necessarily make organizations more secure, but rather require them to expend significant additional resources, only to become more compliant.

When considering the specificity of the Safeguards Rule, it is important to contrast the Rule's application by the FTC, to that of other security requirements established by GLBA for financial institutions. For instance, interagency guidelines established for banks are more prescriptive, appropriately so, because various agencies actively supervise and monitor the activities of the entities they oversee. In contrast, the FTC lacks supervisory examination authority. Therefore, the FTC can only investigate, and if appropriate, take enforcement action against a small percentage of the entities over which it has jurisdiction. The effect of making the safeguards rule more prescriptive in its set of security requirements would place companies in a position of needing to comply with the requirements that may not be applicable and without the appropriate process for entities to explain why that particular requirement may not be necessary or applicable.

The flexible structure of the Rule has not only proven successful over time, but it has also been a critical element to innovation and growth within—and around—the financial services industry. Under this structure, we have seen the burgeoning Fintech industry rise and grow rapidly with innovative new solutions, while ensuring consumer data security. In 2015, the Economist estimated that there were over 4,000 active fintech start-ups.<sup>2</sup> At the

---

<sup>2</sup> S. P. "Why Fintech Won't Kill Banks," The Economist, June 16, 2015, <http://www.economist.com/blogs/economist-explains/2015/06/economist-explains-12>.

same time, many financial institutions are forming strategic partnerships with technology companies.<sup>3</sup>

SIIA urges the Commission to remain cognizant of the diverse and complex nature of the covered entities, and to therefore refrain from making modifications that would shift the Rule towards a prescriptive set of requirements. Further, in addition to maintaining a consistent, principles-based approach in the future, the Rule should reference and draw from the model of the NIST Cybersecurity Framework. Since its inception more than two years ago, the NIST Framework has proven to be an effective, flexible approach to cybersecurity, because it recommends a suite of standards, guidance and best practices, rather than providing a prescriptive set of step-by-step requirements for entities. The breadth and flexibility of this approach has gained strong support from policymakers, technologists and entities increasingly relying on the document's guidance—substantial support was recently demonstrated by participation and feedback from the many workshops and the feedback received by NIST earlier this year.<sup>4</sup>

## **2. The Safeguards Rule Effectively Applies to a Wide Range of Companies.**

The current scope of the Safeguards Rule is sufficiently broad, not only due to the categorization of “financial institutions” that includes entities engaging in “financial activities,” but it also ultimately affects an even wider range of companies. In practice, while the definition of financial activities only directly applies to those activities found to be “financial in nature,” and not specifically “incidental” or “complementary” services, the Rule's requirements are applied more broadly throughout industry to these entities who compete for business on the basis of being able to meet necessary security requirements of financial institutions and consumers.

Therefore, the Rule has effectively adapted over time to apply not only to a narrow set of financial institutions that collect non-public personal information (NPPI) from their own customers, but also to other entities that receive customer information from financial institutions. Even for entities that are not a financial institution as defined under GLBA and the Privacy Rule, they must comply with the Rule's requirements when receiving NPPI from financial institutions—receipt of NPPI from a financial institution is enough to bind an entity to the Safeguards Rule. In many cases, a financial institution has ultimate responsibility for safeguarding customer information it shares with a service provider. In these cases, financial institutions must confirm that their service providers have implemented an effective information security program to protect customer information.

---

<sup>3</sup> “How Banks Are Joining Hands With Fintech Firms to Serve Customers,” Let's Talk Payments, October 15, 2015, <http://letstalkpayments.com/how-banks-are-joining-hands-with-fintech-firms-to-serve-customers/>.

<sup>4</sup> Analysis of Cybersecurity Framework RFI Responses; NIST; March 24, 2016, [https://www.nist.gov/sites/default/files/documents/cyberframework/RFI3\\_Response\\_Analysis\\_final.pdf](https://www.nist.gov/sites/default/files/documents/cyberframework/RFI3_Response_Analysis_final.pdf).

Contractually obligating service providers to use critical safeguards builds a foundation for consumer trust.

Effectively, the Rule's requirements have been applied by a wide range of traditional businesses, such as check-cashing businesses, professional tax preparers, auto dealers engaged in financing or leasing, electronic funds transfer networks, mortgage brokers, credit counselors, real estate settlement companies and issuers of credit cards. More recently, the rise of a robust Fintech industry reveals broad adoption by these cutting-edge companies usually not deemed to be financial institutions, whether they are contractually bound by partnerships with financial institutions or need to voluntarily comply with the Rule's requirements to meet high consumer standards for privacy and security.

Overall, the effect of the Rule has been positive for consumer security, as independent third parties also must take the same critical steps to ensure the safeguarding of consumer data, such as regularly testing and reviewing key controls, systems, and procedures of the information security program to confirm that they control the risks and achieve the overall objectives of the institution's information security program. Their information security programs must be monitored, evaluated, and adjusted in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information security.

As the Commission considers the current scope of the Safeguards Rule and potential modifications to include entities that are significantly engaged in activities that are incidental to financial activities, SIIA recommends that the FTC assess whether the market has demonstrated a gap in application of security standards that warrants such an action.

### **3. The FTC and CFPB Maintain Overlapping Enforcement Jurisdiction of Financial Institutions and Companies Affected by the Safeguards Rule**

While the FTC has maintained rulemaking and enforcement authority for the Safeguards Rule established by the GLBA, recent action by the Consumer Financial Protection Bureau (CFPB) has highlighted overlapping enforcement authority in this area. Specifically, in March 2016, the CFPB issued a consent order against Dwolla, Inc., an online payment platform, alleging that Dwolla represented to consumers that it maintained "reasonable and appropriate" data security safeguards, when in fact it did not.

Under the Consumer Financial Protection Act (CFPA), rule-writing, supervision and enforcement of a wide variety of federal consumer financial laws were transferred from various agencies to the CFPB. These "enumerated consumer laws" include, for example, the privacy provisions of the GLBA. However, although the CFPA altered the Commission's rulemaking authority with respect to the Privacy Rule, it specifically did not

transfer to the CFPB the GLBA data security requirements, and therefore it did not in any way alter the Commission's rulemaking authority for the Safeguards Rule. The Commission formally recognized this outcome in its proposed changes to the Privacy Rule in 2015.<sup>5</sup>

Therefore, the recent CFPB enforcement action, where the CFPB exercises its authority provided by the CFPA to police data security practices in the financial space, utilizing its unfair, deceptive or abusive acts or practices (UDAAP) authority, presents overlapping enforcement authority with the FTC's abilities under the Safeguards Rule. SIIA recommends that the FTC clarify its understanding with respect to overlapping jurisdiction for enforcement authority for financial institutions and companies affected by the Safeguards Rule.

Again, thank you for the opportunity to comment on this important policy review.

Sincerely,

Ken Wasch  
President

---

<sup>5</sup> Amendment to the Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act, Proposed Rule by the FTC, Jun 24, 2015, <https://www.federalregister.gov/documents/2015/06/24/2015-14328/amendment-to-the-privacy-of-consumer-financial-information-rule-under-the-gramm-leach-bliley-act>.