

Before the  
FEDERAL TRADE COMMISSION

Standards for Safeguarding Customer Information )  
Safeguards Rule )  
16 CFR 314 )  
Project No. P14507 )

COMMENTS OF THE NATIONAL BUSINESS COALITION  
ON E-COMMERCE & PRIVACY

The National Business Coalition on E-Commerce & Privacy (“Coalition”) is a coalition of major financial services companies that works for robust and consistent data security, security breach notice, privacy and consumer protection regulation. The Coalition appreciates the opportunity to file comments on the Federal Trade Commission (“FTC” or “Commission”) request for public comment (“RFC”) on the Standards for Safeguarding Customer Information (“Safeguards Rule” or “Rule”),<sup>1</sup> which was promulgated pursuant to the Gramm Leach Bliley Act (“GLBA”).

We urge the FTC to refrain from amending the Safeguards Rule because of the Rule’s continued utility and applicability to financial institutions and FTC regulated entities even after 14 years.<sup>2</sup> The Coalition and its members view the GLBA Safeguards Rule as a model data security regulation. Critically, it is effective while flexible and process-based. Indeed, several states have codified the Safeguards Rule.

The GLBA Safeguards Rule was issued by the FTC in 2002. The Rule implements a standard requiring financial institutions to maintain a comprehensive information security program designed to safeguard the security and confidentiality of customer information, protect against threats or hazards to that security, and protect against unauthorized access. The FTC recognized that the Safeguards Rule should be flexible rather than overly proscriptive in order to allow financial institutions to respond to the changing landscape of security threats, to allow for innovation in security practices and to accommodate changes in technology. As a result, the Safeguards Rule has allowed financial institutions to evolve their security practices to meet and combat constantly changing cyber risks.

The RFC asks both whether the framework should become more specific and whether the Commission should modify the Safeguards Rule to incorporate any information security standards or frameworks. Specifically, the RFC asks whether the Safeguards Rule should incorporate or reference the National Institute of Standards & Technology Cybersecurity Framework (“Cybersecurity Framework”) or the Payment Card Industry Data Security Standards (“PCI-DSS”).

With regard to the first question on whether the rule should be updated to be more specific, it is precisely the high-level, process-based character of the GLBA Safeguards Rule

Axiom Corporation  
Ally  
Bank of America  
Charles Schwab & Co.  
Deere & Company  
Experian  
Fidelity Investments  
General Motors Corporation  
Investment Company Institute  
JPMorgan Chase & Co.  
Principal Financial Group  
The Vanguard Group  
Visa Inc.

Tony Hadley  
Chair

500 8<sup>th</sup> Street, N.W.  
Washington, DC 20004  
202.799.4361  
Fax: 202.799.5361

<sup>1</sup> 16 CFR Part 14.

<sup>2</sup> The Safeguards Rule does not apply to all Coalition members or to all financial institutions.

that have enabled the rule to apply well to small and large organizations alike while keeping up with rapidly evolving threats. It is important that the FTC retain this flexibility.

Coalition members believe that incorporating the Cybersecurity Framework into a static rule would be contrary to purposes of the Cybersecurity Framework and would sacrifice the current benefits of the Safeguards Rule to both consumers and financial institutions. As Michael Daniel, the special assistant to the President and cybersecurity coordinator, explained, the Cybersecurity Framework is intended to remain collaborative, voluntary, and innovative over the long term.<sup>3</sup> Adopting the Framework itself as a rule or attaching any sort of mandatory Framework compliance requirement even if through a simple reference in the Safeguards Rule, would deviate from the voluntary and flexible nature of the Framework as required under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" issued in February 2013 ("Cybersecurity EO") and the Cybersecurity Enhancement Act of 2014, P.L. 113-274. It would also abandon the long standing approach of the Safeguards Rule of allowing financial institutions to adopt security practices appropriate to their own circumstances. Furthermore, the Safeguards Rule in its current form already accommodates use of the Framework so adding a specific reference is unnecessary.

Further, the Commission should definitely not modify the Safeguards Rule to include a reference to or incorporate the PCI-DSS. First, PCI-DSS is a set of security requirements imposed by payment card networks on merchants and others as a condition for use of those networks. It is enforced through severe potential fines as a matter of private contract. Elevating this set of private standards to the force of federal law would create a troubling precedent of outsourcing federal rulemaking to a small group of private parties without any due process protections. Second and furthermore, it is unnecessary because PCI-DSS is already subject to its own enforcement system. Third, PCI-DSS applies only to payment card data, and applying it to other data would project PCI-DSS outside of the purposes for which it was created. Finally, applying the highly specific PCI-DSS Framework would run counter to the Cybersecurity EO, which established the goal of eliminating conflicting cybersecurity regulations rather than creating them.

Finally, adopting requirements to follow the Framework or the PCI-DSS would be a major change in data security law which, given the policy reasons weighing against these changes, would not advance the protection of customer financial information.

Respectfully submitted,

  
National Business Coalition on E-Commerce  
& Privacy

Axiom Corporation  
Ally  
Bank of America  
Charles Schwab  
& Co.  
Deere & Company  
Experian  
Fidelity Investments  
General Motors  
Corporation  
Investment  
Company Institute  
JPMorgan Chase  
& Co.  
Principal Financial  
Group  
The Vanguard  
Group  
Visa Inc.

Tony Hadley  
Chair

500 8<sup>th</sup> Street, N.W.  
Washington, DC 20004  
202.799.4361  
Fax: 202.799.5361

<sup>3</sup> [www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations](http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations).