

November 4, 2016

Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Avenue NW  
Suite CC-5610  
Washington, DC 20580

Re: **Safeguards Rule, 16 CFR 314, Project No. P145407**

The Retail Industry Leaders Association (RILA) welcomes the opportunity to provide comments to the Federal Trade Commission (FTC) regarding the Gramm-Leach-Bliley Act (GLB) Safeguards Rule. It is important for any regulatory agency to solicit feedback on the costs and benefits of their specific rules as well as the economic impact.

By way of background, RILA is the trade association of the world's largest and most innovative retail companies. RILA members include more than 200 retailers, product manufacturers, and service suppliers which together account for more than \$1.5 trillion in annual sales, millions of American jobs and more than 100,000 stores, manufacturing facilities and distributions centers domestically and abroad.

In regards to the question below, this comment letter will specifically outline the serious concerns our members would have in codifying the Payment Card Industry Data Security Standards (PCI-DSS) or incorporating information security standards into the Safeguards Rule.

*Should the Rule 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 or the Payment Card Industry Data Security Standards?*

As a general matter, retailers support market-based voluntary consensus standards organizations such as the International Organization for Standardization (ISO) as well as the work of the National Institute for Standards and Technology (NIST). The standards, frameworks, and guides produced by the open and transparent multi-stakeholder processes run by these organizations are vital to our business. But, reference to standards in regulation or to the NIST Cybersecurity Framework has the potential to chill the vitality of those processes. Standards or frameworks which have the force of law, move from the orbit of the engineer to the lawyer with detrimental effect.

For retailers, the protection of a customer's personal information is of the utmost importance. However, incorporating the PCI-DSS into the Safeguards Rule would not advance retailer efforts, in fact it would be a step in the wrong direction for the FTC and the payment ecosystem.

One of the immediate concerns surrounding this issue is that PCI-DSS is driven by the major card networks who control and implement these policies within the governing apparatus of the Payment Card Industry Security Standards Council (PCI). Preventing retailers from having a defined role at the decision-making level subverts what could be a collaborative working partnership. This is an important aspect and RILA members believe PCI is not a voluntary consensus standards body representative of all the key entities in the payment space. The rules promulgated by PCI are therefore not the products of open and transparent processes and should neither be given the weight of actual standards nor considered as a benchmark or framework for any

information security standards by the federal government.

There is also further cause for concern that PCI-DSS is more of the “check the box” audit without a full understanding of the evolving threats. PCI-DSS would benefit the industry more broadly by focusing on a risk based analysis and developing a greater understanding of the measures retailers are taking to confront these new challenges. This has been highlighted by the merchant community with how PCI treats all infractions equally and we strongly encourage them to alter their approach to truly calibrate for risk. Adopting their current policies and actions into federal guidelines could have a negative effect on consumers and businesses of all sizes.

Once again, there is nothing more important than the protection of our customer’s personal information, which is why retailers were disappointed when PCI did not recommend all the new chip enabled EMV cards come with a personal identification number (PIN). Failure to adopt and implement the easiest deployable security technology at the time, undermines PCI security claims.

In conclusion, RILA strongly urges the FTC to not adopt PCI-DSS or incorporate information security standards into the Safeguards Rule.

Please direct questions or requests for further information about this comment letter to Austen Jensen, vice president for government affairs, at [austen.jensen@rila.org](mailto:austen.jensen@rila.org) or 703-600-2033.

S



Austen Jensen  
Vice President, Government Affairs