



November 21, 2016

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, N.W.
Suite CC-5610 (Annex B)
Washington, DC 20024

Submitted Electronically at <https://ftcpublic.commentworks.com/ftc/safeguardsrulenprm/>

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

The National Automobile Dealers Association (“NADA”) submits the following comments to the Federal Trade Commission (“FTC” or “Commission”) regarding the Commission’s request for comment (“Request”) on its Standards for Safeguarding Customer Information (“Safeguards Rule” or “Rule”).

NADA represents over 16,000 franchised dealers in all 50 states who (i) sell new and used cars and trucks; (ii) extend vehicle financing and leases to consumers that routinely are assigned to third-party finance sources; and (iii) engage in service, repair, and parts sales. Our members collectively employ over 1 million people nationwide. Most of our members are small businesses as defined by the Small Business Administration. Because of the financing and lease activity in which they are engaged, most of our members are “financial institutions” under Gramm-Leach-Bliley, and are therefore subject to the restrictions and obligations under the Safeguards Rule.

We believe that the Safeguards Rule is well-established, generally efficient for financial institutions and consumers alike, and has provided benefit to consumers through its focus on the security and safeguarding of sensitive personal information. Financial institutions are familiar with the Rule, have established practices and policies in reliance on the current rule that provide security and privacy benefits to consumers, and we believe that, for the most part, the Rule should remain as it is, and that any changes should be approached with caution.

I. The Rule Should Include an Additional Focus on Service Providers

One area that has changed since the adoption of the Rule is the “virtual” landscape in which financial institutions now largely operate. While the safeguarding of physical information (in hard copy) has changed relatively little since the Rule’s adoption, the scope and nature of the efforts required to safeguard electronic data have changed tremendously. Consumers are demanding instant electronic access and interface with financial institutions, and financial institutions are generally more reliant than ever on professional IT service providers in every aspect of their business: to store, process, securely transmit, and utilize customer information. These service providers will often then subcontract many of these duties - data storage, for example – to subcontractors¹ who then have access to customer information and must also safeguard that data. The volume of data and the complexity of these networks have grown exponentially. All these changes have been profound, and have unfortunately been accompanied by an increase in the number and scope of efforts by bad actors to impermissibly obtain this information.

While the Rule has, from the start, addressed third parties with access to customer information under the concept of “service provider,” the reality is that the obligations of the Rule, including as to service provider activity, fall exclusively on the financial institution. Service providers: (a) have become virtually indispensable to financial institutions’ business activity; (b) are central in the safeguarding of consumer data; (c) often engage virtually all of the *actual* activity required to safeguard electronic data; and, (d) are often entities that are “in the data business” – both protecting and leveraging data. Nevertheless, these entities ultimately have no direct obligations under the Rule.²

This is true even as we have seen an increasing number of high-profile data breaches and security incidents at both financial institutions and non-financial institutions alike where service providers are the attack vector through which a security incident takes place, and it is often the lack of adequate safeguards at that service provider that leads to exposure of consumer data.

We certainly understand the need for financial institutions to be primarily responsible for safeguarding their data and for continuing to ensure that their service provider contracts contain the required restrictions and obligations under the Rule. However, we believe that changes in the marketplace and the transformed nature and scope of service provider activity – in particular, electronic service provider activity – highlight the need to consider amending the Rule so that it more squarely addresses the critical role service providers play in safeguarding electronic data.

¹ Who then in some cases subcontract to sub-subcontractors.

² There are limitations under the Privacy Rule on a service provider’s ability to reuse or redisclose personal information but, as outlined herein, those restrictions are often difficult for financial institutions to track, audit, or enforce.

This is especially true given the practical difficulty that many financial institutions, particularly smaller financial institutions like most dealers, are beginning to face in properly ensuring compliance by service providers, and service provider subcontractors. For example, certain services, such as data storage or processing, are often only available on commercially reasonable terms from certain large providers. It is our understanding that such large providers often have contracts of adhesion that make it difficult for either the financial institution, or the service provider who must subcontract with that large institution to obtain the appropriate safeguards obligations, audit rights, and other terms needed under the Rule.

In addition, the nature of data itself leads to an asymmetry of information between the service provider and the financial institution with respect to the customer information, so that it is ultimately only the service provider who knows with certainty what they are or are not doing with respect to that data. This makes it difficult if not impossible for a financial institution to establish conclusively through audit or otherwise that the service provider is indeed honoring its contractual safeguarding obligations. This same asymmetry applies as between the service provider and its subcontractors as well.

One of the questions posed in the Request is: “*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?*” We note that among the activities that Board deems to be closely related to banking is “providing financial data processing and transmission services, facilities (including hardware, software, documentation, or operating personnel), data bases, advice, or access to these by technological means.”³

³12 CFR 225.28 (14) Data processing.

(i) Providing data processing, data storage and data transmission services, facilities (including data processing, data storage and data transmission hardware, software, documentation, or operating personnel), databases, advice, and access to such services, facilities, or data-bases by any technological means, if:

(A) The data to be processed, stored or furnished are financial, banking or economic; and

(B) The hardware provided in connection therewith is offered only in conjunction with software designed and marketed for the processing, storage and transmission of financial, banking, or economic data, and where the general purpose hardware does not constitute more than 30 percent of the cost of any packaged offering.

(ii) A company conducting data processing, data storage, and data transmission activities may conduct data processing, data storage, and data transmission activities not described in paragraph (b)(14)(i) of this section if the total annual revenue derived from those activities does not exceed 49 percent of the company's total annual revenues derived from data processing, data storage and data transmission activities.

II. The Rule Should Not Be Modified To Incorporate Outside Standards – Unless It Was to Establish A “Safe Harbor”

The Request asks the following:

- *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? If so, which standards should be incorporated or referenced and how should they be referenced or incorporated by the Rule?*

We do not believe it would be appropriate to modify the Rule to refer to or incorporate third party information security standards or frameworks. We certainly agree that such standards are valuable, and would encourage the application of such standards by financial institutions, and even the recommendation of appropriate standards by the Commission. However, incorporating them into the rule itself – and thereby making them a requisite to compliance with the Rule – would strip away the “flexibility” and “reasonableness” standards that have been the hallmarks of the Rule, and we believe it could be counterproductive.

First, it is unclear how such universal standards would practically apply across all financial institutions (and their service providers.) It is also unclear how commercially available or practical such standards would be for all financial institutions. Dealers vary widely in size, but most our members are small businesses, and expensive, difficult, and unwieldy standards that may go beyond the abilities or needs of many financial institutions would not make sense, and would upset the flexibility upon which the Rule is grounded.

That said, if the Rule was modified to provide for a “safe harbor” to financial institutions that complied with a simple, straightforward, commercially-reasonable set of standards, we would likely consider that to be positive change. In other words, if the Rule were modified so that it continued to provide a flexible standard, but also provided a safe harbor for compliance with the Rule through compliance with a set of objective standards, that would potentially be very beneficial. Of course, the details of any such standards are ultimately dispositive, and the standards must be at the least, simple, straightforward, easy to apply, and commercially reasonable.

The Request refers to two possible standards to which the Rule could refer, the NIST Cybersecurity standards, and the Payment Card Industry Data Security Standards (“PCI-DSS”). We do not believe that it would be appropriate or helpful to incorporate or refer to the PCI-DSS. As a standard promulgated by the payment card industry, PCI-DSS generally applies to entities that process credit card transactions (not all financial institutions do), and those standards are arguably intertwined with specific commercial interests. Automobile dealers are both financial institutions and retailers. The payment card industry has undertaken a number of legislative and

litigation efforts in recent years seeking to transfer the financial obligations related to payment card breaches to retailers. The issue of compliance with the PCI-DSS standards is often an issue in these disputes, and we think it would be highly inappropriate to essentially “require” compliance with these standards via the Rule. This is not only because of the potential conflict between the payment card industry and retailers, but also because the PCI-DSS standards are generally designed for credit card processing security issues, not the more comprehensive data security needed to safeguard electronic data of all types. In addition, it is our understanding that compliance with PCI-DSS standards can require hiring and paying a third party to certify compliance. This requirement would add significant costs to compliance with the Rule that would not be offset by an attendant benefit to consumers.

The NIST Cybersecurity standards are less objectionable as the basis for a safe harbor, but further details would be needed to determine how applicable and commercially reasonable those standards are for all financial institutions.

III. The Rule Should Not Be Modified to Require a Response Plan as Part of the Information Security Program

The Request asks: *“Should the elements of an information security program include a response plan in the event of a breach that affects the security, integrity, or confidentiality of customer information?”*

We do not believe that the elements of an information security program should include a response plan. While we generally agree that it is sensible and often appropriate for financial institutions to prepare an action plan before a data breach occurs, we do not believe it is either required or appropriate under the Rule. Of course, data breaches are governed by state law, and these state laws vary in terms of scope, applicability, and the obligations to affected parties – each of which would necessarily dictate an appropriate response plan. Adding such a new requirement for all financial institutions would add a burden that is not commensurate with any benefit it may provide, and we believe that data breach response and responsibility should remain a function of state data breach laws.

We do agree, however, that continued guidance on these and related issues from the FTC is appropriate. For example, NADA shared the FTC’s recent publication “Data Breach Response: A Guide for Business,”⁴ with our members, and would be glad to continue to work with the Commission to ensure that the latest and best guidance materials are shared with dealers.

⁴ https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf

IV. Conclusion

The Safeguards Rule is an important component in the overall push for data privacy and security that our members undertake. The automotive industry is, along with many others, taking great strides to address these issues both within and outside the regulatory requirements. Dealers certainly share the desire to protect their customer information, and are working hard toward greater protections every day. NADA welcomes the opportunity to work with the Commission, both as part of this Review and elsewhere in addressing the important data privacy and security issues dealers face. Thank you for the opportunity to comment, and please do not hesitate to contact us if we can provide any further information to assist you in your efforts.

Sincerely,

/s/

Bradley Miller
Director, Legal and Regulatory Affairs
National Automobile Dealers Association