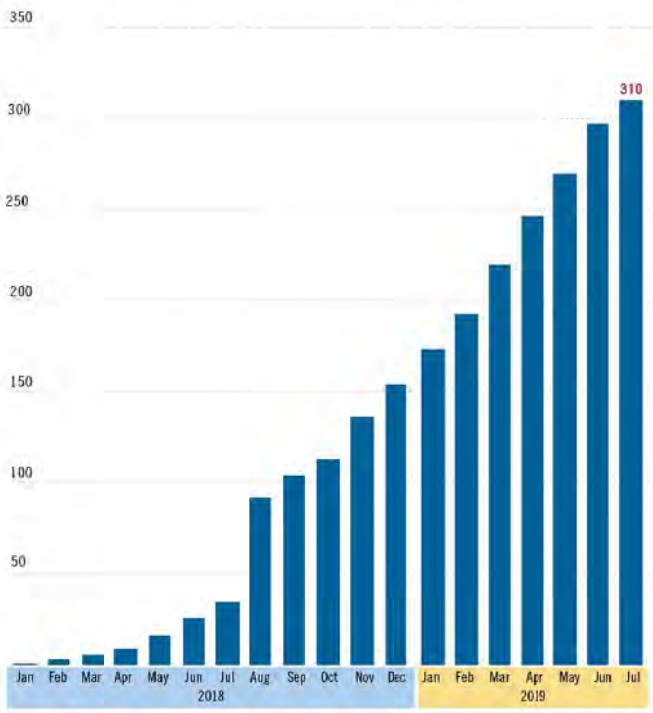
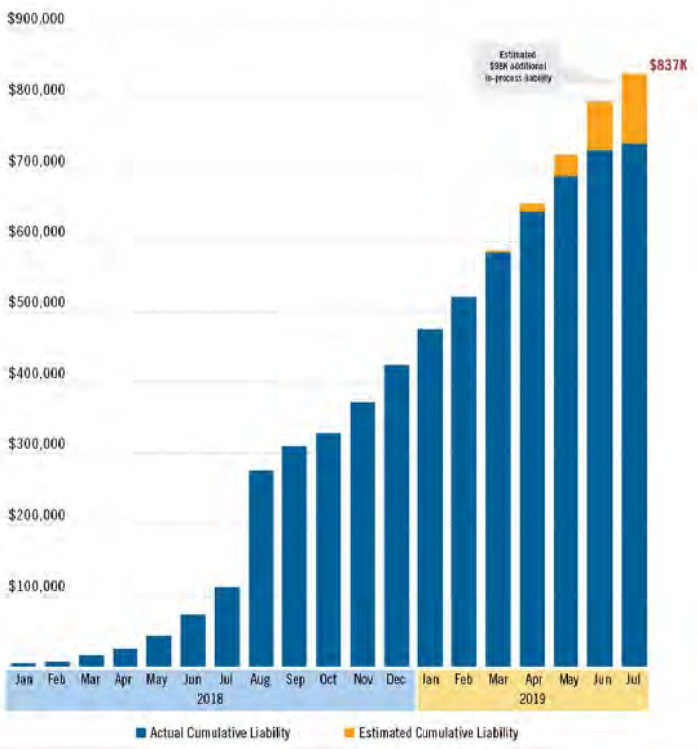
The Effect of DOD Inaction on MLA

(Data from just one of hundreds of finance sources that serve the military)

Cumulative **Number** of Service Members Who Suffered Total Loss of Vehicle **Without** GAP Waiver Protection Since DOD Issued MLA Interpretive Rule



Cumulative **Liability** of Service Members Who Suffered Total Loss of Vehicle **Without** GAP Waiver Protection Since DOD Issued MLA Interpretive Rule



August 12, 2019

Via E-Mail

The Honorable James N. Stewart
Acting Under Secretary of Defense (Personnel and Readiness)
Department of Defense
4000 Defense Pentagon
Washington, DC 20301-1000

Dear Mr. Stewart:

I write to follow up on several letters we have sent to the Department of Defense (DOD)[1] explaining the harm to service members that has been caused by DOD's issuance of Question and Answer 2 of its Interpretive Rule pertaining to the Amended Military Lending Act Regulation (Q&A 2)[2] and to provide recent market data demonstrating the continuing and increasing nature of this harm while Q&A 2 remains in effect.

The first attachment reflects the cumulative number of active duty service member customers of a single finance source who have experienced a total loss of their vehicles without GAP Waiver protection since the finance source ceased taking assignment of credit contracts with service members that included GAP Waiver as a result of DOD's issuance of Q&A 2. (Prior to the issuance of Q&A 2, 81% of the credit contracts purchased by this finance source included optional GAP Waiver chosen by the service member.)

The second attachment reflects the cumulative liability of such active duty service member customers.

These numbers are alarming. Since January 2018 –

1) 310 service members have suffered a total loss of their vehicles without GAP Waiver protection, and

2) they collectively owe $837,000 in connection with vehicles that no longer exist.

[1] See the Joint National Automobile Dealers Association (NADA)-American Financial Services Association petition to DOD to withdraw Q&A 2 dated January 18, 2018; the NADA letter to DOD Principal Deputy General Counsel William S. Castle, Esq. dated October 12, 2018; and the NADA letter to DOD Principal Deputy General Counsel William S. Castle, Esq. dated February 6, 2019.
[2] 82 Fed. Reg. 58,739 – 58,742 (Dec. 14, 2017).

As noted, this is data from just one of hundreds of finance sources that serve the military community. Clearly, the full effect on service members of this situation is much greater. Indeed, as set out in our February 2019 letter to DOD, a conservative estimate of the marketwide impact of DOD's issuance of Q&A 2 is that it has exposed approximately 5,000 Warfighters who purchased and financed vehicles in 2018 to approximately $15 million in liability from total loss occurrences.

Further, as the bar graphs indicate, the loss numbers are rapidly increasing. What adversely affected a limited number of service members in the months immediately following DOD's issuance of Q&A 2 now adversely affects a much greater – and growing – number of service members.

Regrettably, these service members now must contend with two sources of vehicle-related debt: that related to the vehicle they no longer possess and that related to a new vehicle they will have to acquire to satisfy their transportation needs. This presents precisely the type of financial readiness challenge that the Military Lending Act was designed to prevent.

We therefore reassert our and many other organizations' ongoing requests to DOD to move expeditiously to withdraw Q&A 2 before additional harm is caused to the military community.

Thank you for your attention to this matter. Please let me know if we can provide you with any additional information.

Sincerely,

/s/

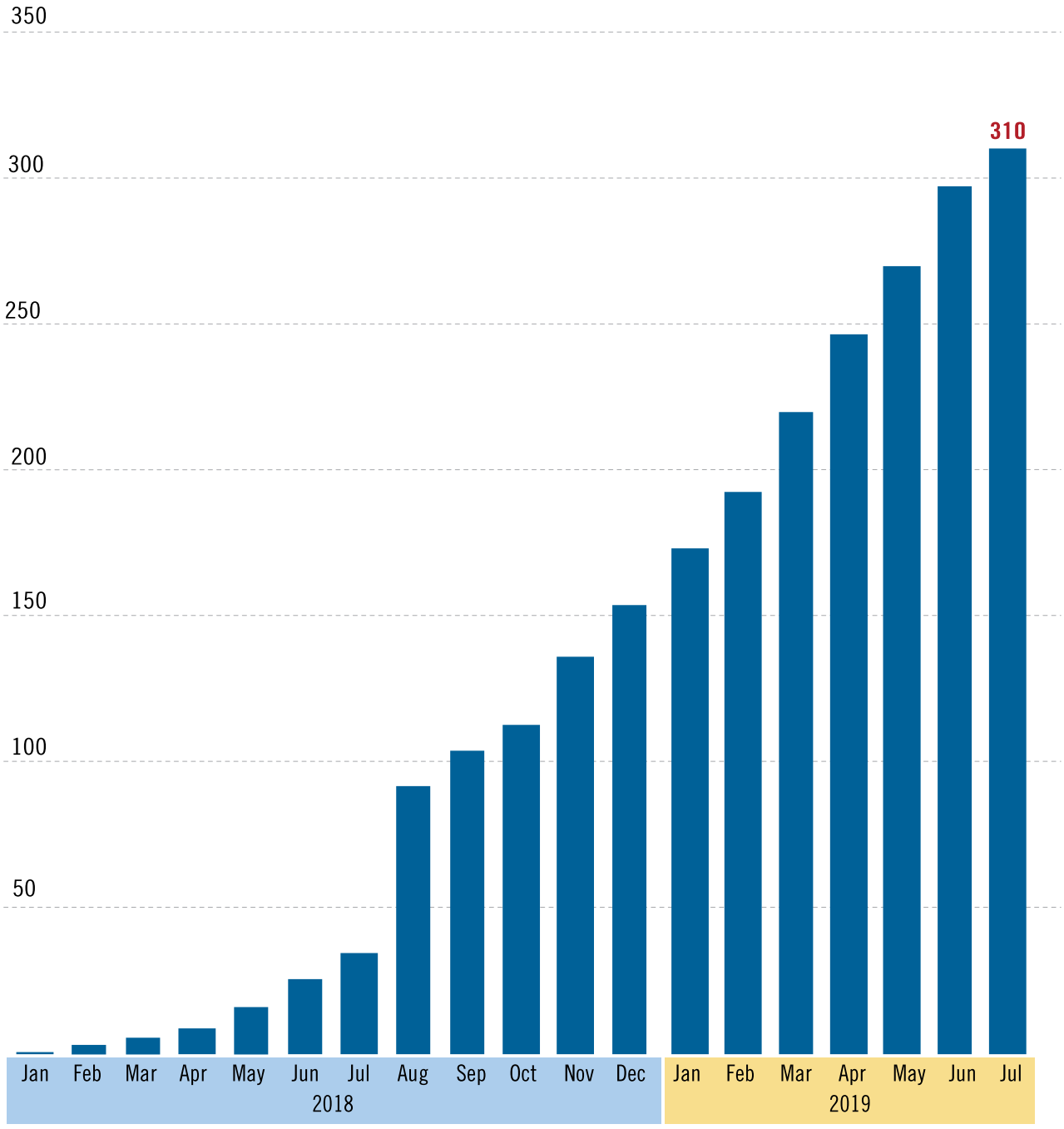
Paul D. Metrey
Vice President, Regulatory Affairs

Cc: The Honorable Mark T. Esper
The Honorable James Michael Mulvaney
The Honorable David L. Norquist
The Honorable Paul C. Ney, Jr.

The Effect of DOD Inaction on MLA

(Data from just one of hundreds of finance sources that serve the military)

Cumulative Number of Service Members Who Suffered Total Loss of Vehicle Without GAP Waiver Protection Since DOD Issued MLA Interpretive Rule



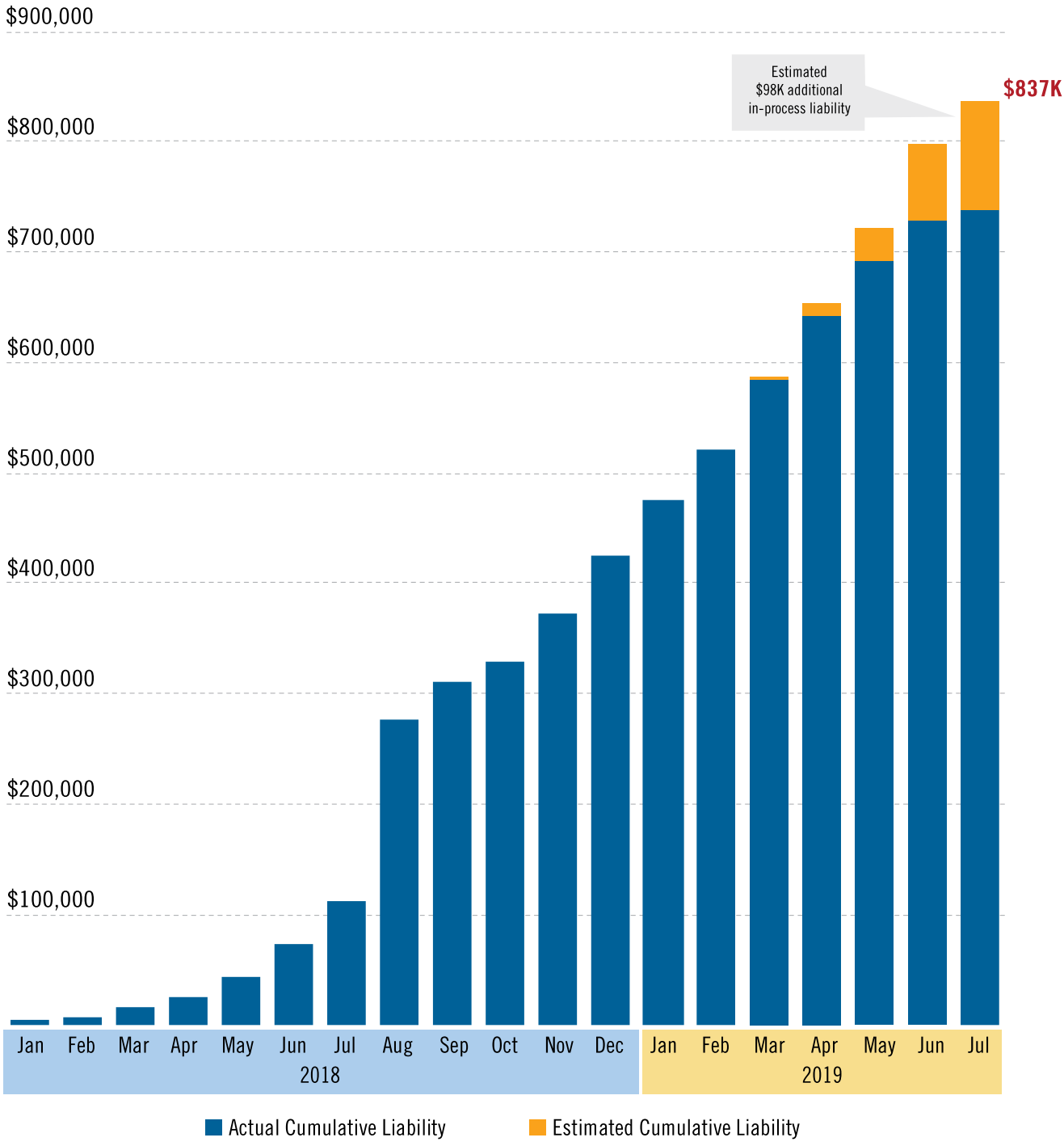
NADA | NATIONAL AUTOMOBILE DEALERS ASSOCIATION 8484 Westpark Drive, Suite 500 | Tysons, VA 22102
nada.org | 800.252.6232

D19-0489.08082109

The Effect of DOD Inaction on MLA

(Data from just one of hundreds of finance sources that serve the military)

Cumulative Liability of Service Members Who Suffered Total Loss of Vehicle Without GAP Waiver Protection Since DOD Issued MLA Interpretive Rule



NADA | NATIONAL AUTOMOBILE DEALERS ASSOCIATION 8484 Westpark Drive, Suite 500 | Tysons, VA 22102
nada.org | 800.252.6232

D19-0489.08092109

August 2, 2019

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

Submitted electronically at https://regulations.gov

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

The National Automobile Dealers Association ("NADA") submits the following comments to the Federal Trade Commission ("FTC" or "Commission"), regarding the notice of proposed rulemaking ("NPRM" or "Notice") to amend the FTC Standards for Safeguarding Customer Information ("Safeguards Rule" or "Rule").

NADA represents over 16,000 franchised dealers in all 50 states who market and sell new and used cars and trucks, and engage in service, repair, and parts sales to consumers and others. Our members collectively employ over one million people nationwide. As our members assist consumers in obtaining financing or leasing options for new and used vehicles, they are generally deemed to be financial institutions under the Gramm-Leach-Bliley Act[1] ("GLB"), and thus are subject to the Safeguards Rule.

The NPRM seeks to modify the Rule in five main ways: (1) by adding provisions "designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program"; (2) by adding provisions "designed to improve accountability of financial institutions' information security programs"; (3) by exempting certain small businesses from some requirements; (4) by "expanding the definition of "financial institution" to include entities engaged in activities … incidental to financial activities;" and (5) by including the definition of "financial institution" and related examples in the Safeguards Rule itself rather than by cross-reference to the Privacy Rule.

[1] 15 U.S.C. § 6801 et. seq.

NADA believes that the current Safeguards Rule has worked well for many years and largely opposes the modifications proposed in the Notice. Our comments regarding several of the proposed changes are outlined below.

First, we provide some background and an overview that is relevant to the overall consideration of the changes proposed in the Notice. Second, we address the changes proposed in the Notice that raise material concerns for our members, addressing each in turn, as they appear in the Notice. We then address several overarching concerns about the proposal, including the small business exemption and the availability of a safe harbor for financial institutions that comply with the new requirements. Lastly, we include a summary of a cost study prepared by an outside Information Technology ("IT") consulting firm that estimates the direct cost to our members arising from these new requirements.

I. Background and Overview.

The United States does not have a federal privacy or data security law of general applicability. Instead, the U.S. approach to date has been to regulate data in certain industries,[2] contexts,[3] or with regard to certain types of individuals.[4] GLB was enacted in 1999 and the Safeguards Rule became effective in 2003 to address concerns with respect to certain categories of information collected by entities engaged in significant financial activity – so-called "financial institutions." The specific concern was that consumers were required to share highly sensitive financial and personal information about themselves with financial institutions in order to obtain a financial product or service ("nonpublic personal information, or "NPI"), and that information could be abused to the financial detriment of the consumer by someone seeking to steal or misuse it. Therefore, GLB requires, *inter alia*, that the entities receiving certain information should be required to take "reasonable" steps to protect NPI. Importantly, the Rule has, from the start, required that a covered financial institution develop and implement an information security program that is "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue."[5] This approach recognizes the important concept that not all financial institutions are the same in size, scale, or the scope of the data they collect and has been key to the success of the Rule to date.

Indeed, many financial institutions, like the vast majority of automobile dealers, are small businesses, with limited staffing, resources, and expertise that must be carefully, strategically, and appropriately deployed to meet the reasonableness standard of the Rule and adequately protect consumer data. Our members range from large, publicly-trade dealership groups with thousands of employees, to small, single-store dealerships with as few as 10-15 employees. Most of our

[2] Such as the Health Insurance Portability and Accountability Act ("HIPAA") for health data.

[3] Such as GLB for information provided in the course of seeking a financial product or service.

[4] Such as children's data under the Children's Online Privacy Protection Act ("COPPA").

[5] 16 CFR § 314.3(a).

members are small businesses as defined by the Small Business Administration. Nevertheless, our members take great care and make substantial investments in money and time to protect the information they obtain and maintain – not just to comply with the Rule, but also because they care about their customers and want to maintain the trust their customers have placed in them.

Motor vehicle dealers are unique among GLB financial institutions in several important ways that we believe are relevant to the Commission's consideration of the proposed amendments. As noted above, most motor vehicle dealers are deemed to be "financial institutions" under GLB because of the nature of the functions they perform for consumers with respect to the financing and leasing of new and used vehicles. However, unlike most other financial institutions, the "financial services" that dealers perform are only a part of what dealers do, and only a small part of the interaction that dealers have with consumers. For example, while dealers obtain credit-related information and assist consumers with financing or lease transactions, they also sell cars to consumers without any financing assistance, either because the consumer purchases their vehicle without financing (as a "cash" purchaser) or obtains financing elsewhere. Dealers also interact with consumers when they service their vehicle, purchase parts, or otherwise interact with the dealership outside of a financing transaction. As a result, only a limited portion of the data that dealerships obtain is protected NPI under the Rule. Most other financial institutions simply do not have these distinctions among their consumers. For a bank or finance company, all consumer interactions are financial in nature and therefore all of the information obtained is likely to be NPI. For dealerships, however, the question is much more complicated - uniquely so in many ways.

This means that dealerships obtain, and dealership systems contain, a mix of data that includes NPI as well as other data that is not NPI. This also means that the exact same type of information obtained by a dealership may or may not be NPI depending on the context in which it was provided.[6] For example, if Jane Smith was shopping for a vehicle and she provided her phone number and name to a salesperson at a dealership, that information in that context would not be NPI, even if she went on to purchase a vehicle from that dealership for cash. However, if that same person provided her name and phone number to a dealership on a credit application in the course of seeking vehicle financing, then that very same information would be NPI and protected under the Rule.

This background and these distinctions are relevant to our comments below.

II. Modification of the Rule to Add "More Specific Security Requirements."

The first "main modification" in the NPRM is the proposal to provide financial institutions with "more guidance on how to develop and implement specific aspects of an overall information

[6] Some of these unique considerations are outlined in the Commission document entitled *The FTC Privacy Rule and Auto Dealers: Frequently Asked Questions*, available at https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-privacy-rule-auto-dealers-faqs.

security program."[7] This "guidance" is not, however, simply guidance, but a set of additional "specific requirements" that financial institutions must meet under the Rule. The NPRM asserts that despite these new requirements, the proposals would somehow continue to allow for "companies to tailor their programs to their size and to the sensitivity and amount of customer information they collect"[8] and that "the Commission does not believe the proposed new requirements would require an overhaul of existing compliance programs."[9] Exactly how these many prescriptive requirements would allow for such individual tailoring is unclear, but what is clear is that many of these new requirements would indeed require significant change for many financial institutions, including dealers, at tremendous additional cost.

a. The Source of the New "Guidance."

The proposed modifications are "based primarily on the cybersecurity regulations issued by the New York Department of Financial Services ("Cybersecurity Regulations"),[10] and the insurance data security model law issued by the National Association of Insurance Commissioners ("Model Law").[11] This raises several concerns. First, neither of these sources were introduced as possible sources of standards in the 2016 request for comments on the Safeguards Rule.[12] In 2016, the Commission asked, *inter alia*, whether standards or frameworks such as those from the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standards[13] would be appropriate for incorporation into the Rule, but did not seek comment regarding the Cybersecurity Regulations nor the Model Law. Most of the comments received opposed the incorporation of these (or any other) frameworks, and while the Notice states that after considering the comments received, "the Commission declines to propose changing the Rule to incorporate or reference a particular security standard or framework,"[14] it nevertheless thereafter adopts large swaths of the Cybersecurity Standards virtually verbatim.

---

[7] NPRM at 13158.

[8] Id. at 13160.

[9] Id.

[10] 23 NYCRR 500 found at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[11] NPRM at 13163.

[12] Safeguards Rule, Request for Comment, 81 Fed. Reg. 61632 (Sept. 7, 2016).

[13] NADA's comments in response to this request opposed the reliance or incorporation of any third-party standard, noting that compliance with a standard may be worthwhile as a safe harbor for financial institutions, if flexible enough to address the differing needs and circumstances of different financial institutions.

[14] NPRM at 13161.

Second, what may be appropriate for entities subject to the New York Department of Financial Services or state insurance commissioners may not be appropriate for entities subject to the Rule, and no explanation or justification has been offered as to why this standard is appropriate nationwide and universally. There does not appear to be any evidence that these standards have proven effective – that is, proof that adoption of these standards has resulted in lower incidents of data breach or that the specific steps that would be required under the Notice have been shown to thwart breach efforts. There has been little time to analyze these sources, and there is no explanation or analysis detailing why these sources, and not others that may exist, are appropriate for application to all financial institutions. The new requirements proposed pursuant to these standards may indeed prove effective, but before they are mandated as broad new requirements under the Rule, data about the experience of entities currently subject to these rules needs to be gathered and analyzed.

b. The Proposed New "Security Requirements."

The Commission's assertion that "the proposed new requirements would [not] require an overhaul of existing compliance programs" may be true for entities already subject to the Cybersecurity Regulations or for larger, more sophisticated financial institutions with greater in-house IT resources and expertise. [15] But as outlined below, it would not be the case for most others, including our members, who are not currently subject to these Cybersecurity Rules.

There are several new security requirements in the Proposal, most of which closely track the Cybersecurity Standards. NADA opposes the majority of these new requirements because we believe that they will largely operate to add tremendous additional costs for our members (and ultimately consumers), without any demonstrated and material gain in cybersecurity protection. These new requirements reflect an unhelpful shift from a prudent reasonableness standard to a set of prescriptive requirements that may make sense for certain entities but are ill-suited to other financial institutions – in particular, for smaller entities, including those above the proposed threshold for exempt financial institutions set forth in proposed section 314.6.

As an initial matter, there is no adequate evidence or support (cited in the Notice or otherwise) for the underlying premise that there is a need to abandon the current, flexible, "reasonableness" approach under which financial institutions have operated for more than fifteen

[15] For example, one large financial institution recently announced that it spends over $600 million per year on cybersecurity with over 3000 employees. See https://www.secureworldexpo.com/industry-news/jpmorgan-chase-cybersecurity-budget It has also recently been reported that the combined cybersecurity budget for "the two biggest U.S. banks — J.P. Morgan Chase and Bank of America — .. ha[s] swollen to a combined $1.4 billion a year," and that "[o]verall, the industry spends an average of $2,300 per employee annually on cyberdefense." See https://www.cnbc.com/2019/07/30/jamie-dimons-worst-fears-for-banks-realized-with-capital-one-hack.html (citing a Deloitte survey released in May, 2019). The notion that a blanket set of requirements that would apply to entities of that size and scope as well as a small dealership makes little sense in our view.

years. Even if there were, there is no analysis or data supporting why these changes would be appropriate or helpful at this time. Furthermore, this NPRM is not driven by any Congressional mandate, nor by any specifically asserted new harm or market reality that requires such extensive changes. Instead, the NPRM is ostensibly a follow-up to the 2016 Commission request for comment on the Rule that the Commission sought as part of its periodic review of rules and guides.[16] The Notice does address the comments received in response to that 2016 request, but the NPRM goes well beyond the issues raised in 2016.

Other than a passing reference to a "rapidly changing cybersecurity landscape,"[17] the Notice contains no justification, reasoning, or data that would support the need for these changes. For example, there is no discussion or assertion that the current Rule is not working, or any indication or data to support the notion that the proposed changes would further the purposes of the Rule within the statutory mandate, or even improve the current cybersecurity landscape for consumers.

Instead, the new requirements are generally justified as "clarifications" of existing requirements under the Rule, and that the proposed changes are "simply mak[ing] these requirements explicit."[18] Repeatedly, the Notice cites to FTC enforcement actions as support for these new explicit requirements.[19] In effect, this Notice purports largely to "codify" in the Rule a series of requirements imposed by the Commission in enforcement action consent agreements against individual entities. As noted in our recent comments in response to the FTC's proposed consent agreement with DealerBuilt,[20] these consent agreements were generally not adjudicated in any neutral forum, were based on a record that was not subject to any public scrutiny, and the steps required in those agreements were reactions to specific fact patterns applicable to the particular entity and circumstances that led to the consent order. While we understand the Commission's desire to identify minimum required steps that financial institutions must take under the Rule, new requirements for *all* financial institutions should not be based on unrelated enforcement actions that may not be generally applicable to all financial institutions subject to the Rule. It is inappropriate to issue such broad and inflexible requirements for entities of all sizes and circumstances, based on unique fact patterns as applied to other entities.

c. Changes since 2003.

---

[16] Safeguards Rule, Request for Comment, 81 Fed. Reg. 61632 (Sept. 7, 2016).

[17] Made by one of the commenters to the 2016 request for comment. 84 Fed. Reg. 13159.

[18] See, e.g., NPRM at 13166.

[19] See e.g., id. fns 86, 88, 90, 92, 95, 96, 98, 102, and 112.

[20] See NADA Comments to the FTC found at https://www.regulations.gov/document?D=FTC-2019-0047-0002

In this regard, it is important to briefly explore what *has* and *has not* changed since 2003 in the context of the Rule.

First, what has not changed over the last 20 years is the basic concept underlying the Rule – that this information is worth protecting, and its basic goal – that entities that collect this information should be required to take reasonable steps needed to protect it. In addition, the nature of the data collected by our members has largely remained unchanged. Most of our members gather today the same basic data in connection with the financial services they provide that they did two decades ago.

In other ways, the context in which this Rule is being considered has seen tremendous change since 2003. First, the tools available to secure sensitive data have proliferated and, in some cases, become more standardized. Cybersecurity is an ongoing "arms race" between those who seek to exploit data and those who wish to protect it. We appreciate that many of the proposed requirements outlined in the Notice reflect the Commission's current position on the basic tools all financial institutions should employ. However, there is simply no evidence in the record that the tools outlined are appropriate, timely, or helpful in protecting consumer data.

Second, the avenues and methods by which this information is now gathered have expanded. In 2003, most of the consumer interaction was in-person and face-to-face. Now, digital and online interaction is the norm. This means that the systems that gather and store this information have increased in number, and the complexity of the data ecosystem in which that data resides, and through which it must be shared, has exploded. Since the adoption of the Rule, financial institutions have moved to largely operating in a "virtual" landscape. 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 undertaken to safeguard electronic data have changed tremendously. Consumers are demanding instant electronic access and interfaces 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 subcontract many of these duties – data storage, for example – to subcontractors 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. All of this complicates data security to be sure, but it would also make compliance with prescriptive rules like those outlined in the Notice far more complicated, difficult, and expensive.

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, continue to fall exclusively on the financial institution. At the same time, technology service providers: (a) have become virtually indispensable to financial institutions' business activity; (b) are central in the safeguarding of consumer data; (c)

often perform *virtually all* of the *actual* activity required to safeguard electronic data; and (d) are generally entities that are "in the data business" – both protecting and leveraging data. 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 it is or is not doing with 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 can exist as between the service provider and its subcontractors, so that the notion of a financial institution – especially a smaller financial institution – possessing full insight into data flows becomes tenuous at best. Nevertheless, these entities ultimately have no direct obligations under the Rule.

Third, the reported incidents of data "breaches," among institutions of all types – including financial institutions – have increased dramatically, as has the profile of those breaches. There is nearly universal agreement that data breaches are impossible to prevent 100% of the time.[21] Financial institutions certainly do not want a data breach and when one occurs, they themselves are victims, along with their customers.[22] Moreover, in many (if not most) of these breaches, the vulnerability that has been exploited arises from issues with service providers or other third parties, not the financial institutions themselves. We agree that the tide of data breaches needs to be stemmed but placing the proposed new requirements outlined in the Notice solely on financial institutions will not have that effect. In addition, many of the new requirements are administrative or *ex post facto* requirements that are designed to assign responsibility rather than prevent data breaches - which is and should be the purpose and primary focus of the Rule.

Fourth, it must be noted that the unique sensitivity of NPI under the Rule has, if anything, *decreased* dramatically over that same time. So-called "Big Data" is a behemoth that has grown beyond the imagination of 1999. It is increasingly rare for Americans *not* to voluntarily and repeatedly share their names, addresses, birthdates, employers, and other basic information that constitutes the vast bulk of NPI[23] with third parties of all kinds. This type of information is available on social media, from public records and other Big Data sources and, in our industry, increasingly from the vehicle itself. Once this information is shared with an entity that is not a

---

[21] See, e.g., NIST SP800-184, Guide for Cybersecurity Event Recovery ("There has been widespread recognition that some of these cybersecurity (cyber) events cannot be stopped and solely focusing on preventing cyber events from occurring is a flawed approach.") Found at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

[22] See, e.g., https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html; https://www.nytimes.com/2019/07/22/business/equifax-settlement.html; https://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/

[23] At least the vast majority of the types of NPI that are routinely obtained by automobile dealers.

financial institution,[24] it becomes almost immediately and virtually universally available. Of course, once it is available, it is difficult, if not impossible for it to be made "unavailable." The amount of information obtained and available from data brokers, social media companies, and others is so vast that, in many cases, third parties who seek this information (for good or ill) can obtain it easily, with or without the consumer's knowledge or consent. While there may be certain categories of information (like Social Security or credit card numbers[25]) that remain the general exception to this new rule, even this information is becoming increasingly available to those who seek it. The available data is so vast that with only one or two pieces of information about an individual – even information such as name and address – it is simple to re-engineer nearly all of the additional information – public or "nonpublic" – that a financial institution like a dealership would ever obtain from a consumer.

The fact that so much of this information is now virtually publicly available means that the *unique* sensitivity of the information obtained by financial institutions has diminished dramatically. We are not advocating against the continued need for the Rule, indeed we support the need to take reasonable steps to protect the NPI that dealers and other financial institutions have. Nonetheless, the new reality regarding the availability of data must be recognized as part of the cost/benefit analysis of the proposed new requirements in the Notice. In other words, any analysis of the wisdom and efficacy of a new requirement that would cost financial institutions writ large $X billion per year must take into account the fact that the cybersecurity "return" on that investment may be marginal as a practical matter as it may have only a marginal effect on protecting information that is not already widely available.

The point here is not to say that information obtained by financial institutions should not be protected – it should. However, this new data reality is relevant to the Rule, and to the *reasonableness* of the steps financial institutions must take to protect the data they collect. It is also relevant to the Notice because while this analysis may be true of the bulk of the information collected and retained by dealers, it may not be true of other financial institutions that collect and maintain other, more highly sensitive and truly nonpublic information. *That is yet another reason why a flexible approach is so critical*, and why it has worked so well for many years.

Whether or not the Commission ultimately adopts some or all of the prescriptive new requirements in the Notice, we would urge the Commission to recognize, within the scope of its authority, the changing nature of this information and the fact that the current definition and understanding of "personally identifiable financial information"[26] and "Nonpublic Personal

[24] Or another entity with regulatory obligations such as a covered entity under HIPAA.

[25] Credit card numbers, while highly sensitive and valuable, are generally not NPI (at least at a dealership) as they are not provided by a consumer in the course of seeking financing.

[26] 16 CFR Part 313(o)(1).

Information"[27] are very broad and may not reflect the types of truly sensitive financial information the Rule was intended to protect.

Lastly, this new "Big Data" reality has led to an understandable backlash, along with legislative efforts to address privacy and security-related concerns, such as the European Union's General Data Protection Regulation and state efforts such as the California Consumer Privacy Act. The Commission recently noted that, "[it] understands that both Congress and the Administration are considering federal privacy legislation." [28] The Commission noted its "strong[] support [for] those efforts," and that "[a]ny legislation should balance consumers' legitimate concerns about the protections afforded to the collection, use, and sharing of their data with business' need for clear rules of the road, consumers' demand for data-driven products and services, and the importance of flexible frameworks that foster innovation."[29] We agree with the continued need for flexible frameworks, like that currently available under the Rule. Moreover, because these federal efforts are being undertaken in earnest now, we agree with the dissenting Commissioners that many of the proposals outlined the Notice are "premature"[30] given the proposed legislative responses to consumer concerns about the use and abuse of consumer data.

d. Cost Analysis.

While the need for the changes outlined in the notice remains unclear, what is clear is that the proposed changes would add material costs for financial institutions which would, by necessity, also increase costs for consumers. In response to this Notice, NADA engaged a third-party IT services firm to conduct a cost analysis of the requirements outlined in the Notice. In conducting this analysis, the third-party IT consulting firm conducted onsite interviews with dealership executives and/or their representatives to review their IT environments, and analyze their IT systems and capabilities, current IT costs, and the potential cost impact of the changes outlined in the Notice for our members. We also received estimates from the IT services firm and several competing firms for the costs associated with outsourcing the duties for each of the new requirements, based on their experience and expert opinion. The cost estimates we received include the estimated up-front, one-time costs, as well as any recurring costs resulting from the changes proposed in the Notice, calculated annually. This expert market experience and insight combined with the information received from dealers provide the source of the cost estimates reflected herein. While it is difficult to determine exactly which, or how much of these cost estimates represent new costs for dealers or other financial institutions, the cost estimates herein

[27] 16 CFR Part 313(n)(1).

[28] https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf (at p.20)

[29] Id.

[30] NPRM at 13177.

represent a best estimate at the additional costs that would be imposed by the new requirements outlined in the Notice. A summary of the results of that analysis is found at Appendix A.

As demonstrated by this analysis, the costs associated with these proposals would be prohibitively expensive. While: (a) many financial institutions may already take many of the steps outlined in the Notice (or steps similar in scope and purpose), and; (b) many of the new requirements could promote the security of data (although this is not established in the record), the security benefits that may be realized by some of these new requirements are not commensurate with the costs that financial institutions would incur to meet them.

In addition, these costs must be viewed in light of the size, structure, and business model of our members. While the numbers reflected in the cost analysis may be easily absorbable by a large, multi-billion-dollar financial institution, it will be prohibitive for many, if not most of our members, who simply do not have the revenue structure, or the margins to absorb costs of this nature and scale. This could lead to tremendous pressure on many of our members and could ultimately reduce competition and consumer choice.

The Safeguards Rule has worked well for over 15 years because it is flexible, and flexibility remains the key to addressing the cybersecurity challenges faced by financial institutions like our members. We urge the Commission to continue to encourage flexible frameworks like the one that has been in place for over 15 years in the Rule to allow financial institutions of all sizes to continue to compete in the marketplace while protecting sensitive consumer information, rather than imposing the series of prescriptive – often ill-fitting – requirements outlined in the notice.

e. Comments on Specific Sections.

Our specific comments to the proposed changes are outlined below:

i. Proposed Amendment to Section 314.2 Definitions.

There are several questions that need to be answered about the proposed new definitions.

1. "Authorized User."

First, the term "authorized user" in proposed Section 314.2(b) is unclear. For example, is the reference in 314.4(c)(3) to "authorized individuals" intended to refer to "authorized users?" If not, how does an authorized individual differ from an "authorized user?"

Also, what does it mean to "participate in [the financial institution's] business operations?" Are financial institutions required to restrict access to their systems and data to anyone who is not an "authorized user?" Would that apply to third party service providers or others with permission to access the systems or data of the financial institution? For example, financial institutions commonly allow access to or share certain data from their systems via API or similar interfaces. Would that sharing need to be restricted to "authorized users?" If so, then the definition itself is too limited as such sharing is likely to occur with entities that do not "participate[] in [the financial institution's] business operations" – at least as that is generally understood. Would such sharing need to meet the multi-factor authentication and other requirements "for any individual accessing

customer information,"[31] or only for those "accessing [the financial institution's] internal networks?"[32] These are just a few of the questions that would need clarification.

2. "Security Event."

The definition of "security event" in proposed Section 314.2(c) also raises questions and concerns. As addressed in our comments regarding the proposed requirement for an incident response plan, *infra,* we are concerned about requirements that are not directly related to protection of the confidentiality or security of consumer information. The inclusion in this definition of "disruption or misuse" of an information system makes this definition overly broad because it is not directly related to the protection of customer information. There are many potential instances where a system can face disruption or misuse that do not implicate the security of the data in the system or present little to no risk of unauthorized access to any data, much less sensitive or protected data.

We also disagree with the decision to "not include the Model Law's exemption for the acquisition of encrypted information or events where the covered entity determines that the information accessed by an unauthorized person has not been used or released and has been returned or destroyed."[33] The Commission states that this was not included because "the Commission believes that a financial institution should still engage in its incident response procedures to address the failures in its information security that allowed such events to occur."[34] First, we would suggest that it is only an information security "failure" under the Rule if personally identifiable data is exposed. Indeed, the entire point of requiring encryption of the data is to prevent exposure that could be harmful to consumers.

Second, it is unclear why a financial institution should be required to "engage in its incident response procedures" to address an issue that has not resulted in a risk to consumers. Just as it would not make sense to require an entity to respond in some formal way to every failed intrusion effort or phishing attempt, it does not follow that a financial institution should be required to engage in expensive and complicated internal procedure to address every "disruption" of their systems where that disruption did not result in any exposure of protected consumer data.

Of course, financial institutions are likely to consider such disruptions, as is reasonably needed, when engaging in and updating their risk assessments. However, the touchstone for blanket requirements like this should be material risks to the security of the data, and therefore we

[31] Proposed 314.4(c)(6).

[32] Id.

[33] NPRM at 13164 at n. 71.

[34] Id.

suggest that the definition include the language exempting encrypted information from the Cybersecurity Regulations noted above, or that other language (such as: "*that exposes or is reasonably likely to subject unencrypted consumer data on the information system to exposure*") be added at the end of the definition of "security event."

3. "Encryption."

In the context of the proposed definition of "Encryption" in Section 314.2(e), we note that most states refer to or define "encryption" in their state data breach laws,[35] and many of those definitions do not require a "protective process or key." The Notice suggests a flexible approach to encryption, but for that to be feasible, we would urge the inclusion of language that would allow for such differences. For example, the definition could include: "…*or securing information by another method that renders the data elements unreadable or unusable*."[36]

4. "Financial Institution" – Addition of "Finders."

NADA supports the proposal in the Notice to amend the definition of financial institution to include entities that are "significantly engaged in activities that are incidental" to financial activities, which would add "finders" into the definition of financial institution and thus make "finders" subject to the Rule.[37]

Acting as a "finder" includes "bringing together one or more buyers or sellers of any product or service for transactions that the parties themselves negotiate and consummate."[38] This "includes providing any or all of the following services through any means:

(a) Identifying potential parties, making inquiries as to interest, introducing and referring potential parties to each other, and arranging contacts between and meetings of interested parties;

(b) Conveying between interested parties expressions of interest, bids, offers, orders and confirmations relating to a transaction; and

---

[35] See, e.g., Colo. Rev. Stat. 6-1-716(1)(d), ("Encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.").

[36] See, e.g., Mich. Comp. Laws 445.63(3)(g) ("Encrypted" means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable.").

[37] NPRM at 13162-63.

[38] 12 CFR 225.86(d)(1).

(c) Transmitting information concerning products and services to potential parties in connection with the activities described in [the two paragraphs above]."[39]

Examples of finder services include:

(a) "Hosting an electronic marketplace on [an] Internet web site by providing hypertext or similar links to the web sites of third party buyers or sellers.

(b) Hosting []the Internet web site of -

a. A buyer (or seller) that provides information concerning the buyer (or seller) and the products or services it seeks to buy (or sell) and allows sellers (or buyers) to submit expressions of interest, bids, offers, orders and confirmations relating to such products or services….

(c) Operating an Internet web site that allows multiple buyers and sellers to exchange information concerning the products and services that they are willing to purchase or sell, locate potential counterparties for transactions, aggregate orders for goods or services with those made by other parties, and enter into transactions between themselves.

(d) Operating a telephone call center that provides permissible finder services."[40]

Using the definition above as a guide, there are many entities that provide finder services for motor vehicle dealers. For example, many companies seek to connect consumers interested in purchasing or leasing a vehicle with a dealer. Third-party lead providers, vehicle inventory hosting websites, automotive financing websites, and many other similar service providers proliferate in the marketplace. Those sites generally obtain consumer information – either via the internet or telephone – that they may share with the dealership in connection with a proposed vehicle financing transaction. While the details vary such that the activity may or may not fall into a definition of "finder," this is relatively common in the automotive market.

Our support for this change should be viewed as part of an overall concern about third-party access to customer information. As outlined above and in our previous comments to the Commission, we believe that placing the exclusive data security requirements on the financial institution under the Rule, to the exclusion of all of the other third parties with access to sensitive data, has led to many of the gaps in security that we have seen over the past years. We 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, changes in the marketplace and the transformed nature and scope of service provider activity – in particular, electronic service provider activity – highlight

[39] Id. at (i)(A)-(C).

[40] Id. at (ii)(A)-(D).

the need to consider amending the Rule so that it more squarely addresses the critical role service providers and other third parties play in safeguarding electronic data.

This is especially true given the practical difficulty that many financial institutions, particularly smaller financial institutions like most dealers, experience 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 viable 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 its service provider who must subcontract with that large institution, to obtain the appropriate safeguards obligations, audit rights, and other terms needed under the Rule, and under the proposed new explicit requirements for all financial institutions regardless of size or market power.

Simply put, it is virtually impossible for a small dealership to dictate contract terms, audit rights, terms of access, *or anything else* to a large technology company with which it does business or with which one of its service providers does business.[41] By way of real-world example, a single point automobile dealership with 15 employees in rural South Dakota does business with a computer company providing ERP services to the dealer.[42] That computer company stores the data for the dealership on the "cloud" with a large cloud provider – say Amazon or Microsoft.[43] That dealership is simply not going to be able to acquire, much less *require*, audit rights with respect to their data in the contract with a multi-billion dollar data storage company. At the same time, that dealership is unlikely to have any real practical choice whether to allow its data to be stored with such an entity. First, the cost advantages of this storage method over in-house servers may make it prohibitively expensive for that dealership to make any other choice. Second, the dealership may not even have a contract with the cloud storage company, but one or more of their IT service

[41] We do not believe it is appropriate to place requirements on financial institutions that many cannot meet.

[42] Enterprise Resource Planning ("ERP") are the systems and software packages used by organizations to manage day-to-day activities, such as accounting, procurement, and manufacturing. In the automotive dealership market, the ERP services are provided by companies that provide systems called Dealer Management Systems, or DMS.

[43] This is, of course, only by way of example, but Amazon Web Services, which is the division of Amazon that provides cloud computing services, is one of the largest providers of such services, with over $30 billion in annual revenue. We make no assertion about Amazon or any other specific provider, but it is our understanding that the contracts for services like these from the larger providers have historically been difficult, if not impossible, to negotiate, much less to impose requirements such as audit rights.

providers may store their data with a cloud provider, and so the dealership may not even have any direct contractual relationship under which they can include the required audit rights.[44]

We support the inclusion of "finders" under the definition of "financial institution," but would urge the Commission to expand on the consequences of this designation,[45] and to explain what this designation means for financial institutions who deal with these "finders." What is the relationship of a financial institution, like a dealer, with a finder that shares NPI with that dealer? Can an entity be a financial institution ("finder") and, at the same time, a service provider for another financial institution with respect to that same data? Do financial institutions who obtain NPI from "finders' need to have the requisite service provider contract language – or is it the other way around, would the recipient financial institution be acting as a service provider to the "finder?"[46]

In this context, we would also urge the Commission to consider other ways of expanding the tools that financial institutions have – particularly smaller financial institutions – with respect to third parties to enable these financial institutions to meet the requirements under the Rule in circumstances where they do not have the requisite market power.

---

[44] Anecdotally, it is our understanding that this type of example is increasingly common, even with larger companies. As macro services like cloud storage become almost ubiquitous, entities of all sizes face similar challenges, with reports that even the largest of companies are not able to request, much less dictate audit rights or similar terms in the contracts with these providers. (See, e.g., https://www.computerworlduk.com/cloud-computing/5-key-legal-considerations-when-negotiating-cloud-contracts-3637604/; https://www.cio.com/article/3096749/5-tips-on-negotiating-a-cloud-agreement.html.)

[45] For example, does this mean that a finder would itself be subject to all of the requirements under the Safeguards Rule, or only limited requirements? Would a finder therefore also be subject to the requirements for financial institutions under the Privacy Rule (such as sending privacy notices), or is this designation somehow limited to the obligations under the Safeguards Rule?

[46] These questions about the relationship between financial institutions are particularly acute in light of the recent enforcement action taken by the Commission against DealerBuilt/LightYear Dealer Technologies, where the Commission alleged that DealerBuilt, a technology service provider to dealers, *is* a financial institution, not as a finder, but simply as a consequence of the fact that they are "significantly engaged in data processing for its customers, auto dealerships that extend credit to consumers…" See Complaint at ¶ 23, *In re LightYear Technologies, Inc.,* No. 172 3051 (June 12, 2019). This allegation raises significant compliance questions for dealers and other financial institutions with respect to their relationship with their service providers and we would ask that the Commission expand on the consequences of this designation and the scope of this expansion of "financial institution." Such clarification is needed, in particular, given this pending analysis of the expansion of the definition of financial institution to "finders."

ii. Proposed Paragraph (a) - Appointing a CISO to Increase Program Accountability.

Proposed Paragraph (a) purports to "expand" the current requirement that a financial institution designate a program coordinator for its information security program under the Rule. This new requirement is more than an expansion. Rather, it would impose a completely new and overly broad requirement on financial institutions to "designate a single qualified individual responsible for overseeing and implementing the financial institution's security program and enforcing its information security program"[47] In other words, it would require financial institutions to hire a qualified Chief Information Security Officer ("CISO"). The stated reason for this new requirement is to "ensure that a single individual is accountable for overseeing the entire information security program and to lessen the possibility that there will be gap in responsibility between individuals."[48]

We oppose this requirement, which will be very expensive for the vast majority of our members and add no demonstrated cybersecurity protection. This is a massive new requirement for financial institutions like our members – even our largest members. In surveying our members, several trends became clear. First, almost none of our members currently have a CISO, so this would be a new cost for all our members. Second, most of our members, even many of the largest of our members, would be likely to outsource this function rather than staffing it internally.

For one thing, the cost of hiring a full-time, "qualified" CISO is prohibitively expensive for most of our members. While it is difficult to determine with any precision, and would differ across the country, there was consensus among our members that the estimated salary for hiring a "qualified" CISO for a dealership could easily exceed $150,000 or more.[49] Even outsourced CISO

[47] NPRM at 13165.

[48] Id.

[49] According to Glassdoor, the average annual CISO salary is over $180,000. *See* https://www.glassdoor.com/Salaries/ciso-salary-SRCH_KO0,4.htm. A 2017-18 industry survey provides

services are very expensive. Reports from our members reported costs ranging from $5,000-$10,000 or more *per day* for CISO consulting services. Our cost analysis found at Appendix A - which assumes outsourcing of this CISO function - reflects a very conservative estimate of $27,500 in average up-front costs for this requirement, with an additional $51,000 per year per dealership if this proposed change were adopted.[50]

While dealers incur some costs associated with the time spent by the currently designated program coordinator, the Notice also requires that if a financial institution outsources the CISO function, it must nevertheless also "designate a senior member of its personnel to be responsible for direction and oversight of the CISO."[51] This new requirement would, in itself, add significant costs to this requirement. Who exactly is this "senior member" going to be? It would, by necessity, be someone with the training and expertise to be able to oversee and direct an outside IT expert. Most dealers do not have any such person on staff. As a result, even if they did outsource the CISO function, they would likely be in a position where they *still* need to hire a new senior member of their staff with IT expertise. And it would need to be someone not only knowledgeable enough to supervise IT experts, but someone willing to accept the responsibility for the actions of the CISO – because "even when the financial institution outsources the CISO function, the financial institution retains responsibility for its own information security,"[52] and "a single individual is accountable for overseeing the entire information security program" at the financial institution. This will not be inexpensive. Indeed, for many of our smaller members, for example in rural areas

---

a higher number – ranging from over $200,000 to well over $300,000 a year. See:

Table 1. CISO Salary Data

	Market Median: 25th Percentile	Market Median: 50th Percentile	Market Median: 75th Percentile
Annual Base Salary	182.4	210.0	254.3
Total Cash Compensation (i.e., base salary plus annual incentives/bonuses)	208.2	253.0	337.1

U.S. national data (across all participants). From 2017 U.S. Mercer Benchmark Database: Mercer/Gartner Information Technology Compensation Report. Data effective date: 1 March 2017 (in hundreds of U.S. dollars).

Source: Gartner (February 2018)

[50] See Appendix A.

[51] NPRM at 13165.

[52] Id. at 13165.

of the country, it will be impossible as there may not *be anyone* available in the local workforce capable of meeting this requirement.

This new "expansion" of the Rule is clearly a significant – indeed a prohibitively expensive – new cost that financial institutions of all sizes[53] would need to incur. While it may help centralize "accountability," there is no demonstrated need for, nor any security benefit from, such centralized "accountability." It may help to have one person responsible if a security event occurs but, as noted above, the touchstone for the Rule is whether it helps keeps data secure, not whether it may assist in determining accountability after a breach occurs.

There are also many open questions that would need to be answered about the scope of this requirement. For example, what does it mean to be a "qualified" expert and how can a financial institution determine if an outside third party is indeed qualified? How exactly would an outside third-party "oversee and implement" a financial institution's security program? Of course, an employee given the requisite authority could do so, but is a financial institution required to turn over the authority to run such a critical function, which could have a serious and material impact on the operations of the business, to a third party? If the third party wished to implement a program that the financial institution deemed to be unreasonable, would they still need to follow that outsourced CISO's direction? Given that the Notice would also require that the program be based on a written risk assessment,[54] must the financial institution allow the CISO to be involved with that assessment? Must the CISO write the assessment? Each of these would add significant costs beyond what is outlined above.

And all these costs are in addition to the explicit new requirement in proposed paragraph (i), discussed below, requiring that the CISO submit a written report at least annually to the board of directors or other governing body of the financial institution, on the status of the program and material matters requiring attention. Our cost estimate for this report alone is approximately $9,000 per year.[55]

iii. Proposed Paragraph (b) – Requiring that the Information Security Program Be Based on a Written Risk Assessment.

Proposed Paragraph (b) requires that the financial institution's information security program be based the findings of its risk assessment and that the risk assessment not only be

[53] While there may be some economies of scale for our larger members, such that the cost per store would be more manageable, it is also clear that the CISO costs – outsourced or not – are higher for larger operations.

[54] See proposed Paragraph (b), discussed *infra.*

[55] See proposed Paragraph (i), discussed *infra*.

written, but that it must "describe how the financial institution will mitigate or accept any identified risks and how the financial institution's information security program will address those risks."[56]

It would also "add a requirement that financial institutions 'periodically perform additional risk assessments'" that reexamine the reasonably foreseeable internal and external risks to the customer information they have and "reassess the sufficiency of any safeguards in place to control these risks."

We oppose these additional new requirements outlined in the Notice related to the risk assessment requirement because they will add significant costs without a demonstration of material improvements to the security of customer information. First, the requirements in proposed Paragraph (b)(1) are well outside the scope of expertise of anyone but the most sophisticated IT professionals. This means that, to conduct and memorialize each of the components of this expanded assessment requirement, the financial institution must engage a qualified IT professional. Does that mean that this written assessment be performed by the CISO? As noted above, many financial institutions will outsource the CISO function (including most of our smaller members) and adding this to the outsourced CISO's duties will add significant cost.

Furthermore, what is the purpose of the requirement that the financial institution "mitigate or accept" identified risks. When is it appropriate to "accept" such risks versus mitigating them? Can that be the result of a reasonable cost/benefit analysis by the financial institution? If not, why not? Requiring documentation of the decision to "accept" identified risks does little to protect data, but it will, of course, create a record that can be distorted and second guessed after the fact. Making decisions like these always requires a context and judgment. That context is lost when it is written and reviewed after an incident has occurred or is alleged to have occurred.

Lastly, what is the measure for the "additional risk assessments?" How often must they be undertaken? Based on what? What are the criteria?

Our cost analysis for this written report requirement is an up-front cost of $26,500, with an additional $26,500 per year per dealership. (See Appx. A)

iv. Proposed Paragraph (c) – "More Detailed" Required Safeguards.

Proposed Paragraph (c) contains a series of prescriptive requirements with which financial institutions would be required to comply. The Notice states that "most financial institutions already implement" these measures and that "this simply makes these requirements explicit in order to clarify the Rule and ensure that financial institutions understand their obligations under the Rule."[57] The source and authority of this assertion is unclear, as many financial institutions do not currently implement some or all of these measures.

[56] NPRM at 13165-6.

[57] Id. at 13166.

One overarching practical concern with respect to several of these requirements is what exactly it means to comply. In other words, in a world where virtually all IT functionality is outsourced to third party IT service providers, how *exactly* will a financial institution ensure compliance with these new requirements? In most cases, a smaller financial institution like an automobile dealership does not *itself* store or protect anything. Indeed, with the ubiquity of services like cloud data storage, even the largest financial institutions often do not house and protect their data themselves. Instead, they engage the services of third parties who engage in these efforts on their behalf. While there are some larger dealers who have in-house IT staff that may actually oversee many of these tasks, even with our largest members, it is ultimately third parties that will actually store the data and be engaged to undertake all of these efforts. This is true of many, if not all of the IT functions undertaken by most financial institutions. In that world, how will a financial institution ensure compliance with these new measures?

The encryption requirement (in proposed Paragraph (c)(4) outlined below) is illustrative. Financial institutions would be required to "encrypt all customer information both in transit and at rest."[58] But what does that mean exactly? Presumably, one thing it means is that the data stored in the financial institution's ERP must be encrypted when stored in that internal system.[59] But how *exactly* does a financial institution like a dealership meet that obligation with the entity providing that service? How does it demonstrate that it has met that requirement? Is it enough that such a requirement is contained in the contract? Is that required? Does the dealership have to take steps beyond a contract to confirm that the data is encrypted? How would they do that? Are they required to hire a third-party IT consultant to audit for encryption? How often? Would it apply to hardware and software? Would it apply to the ERP/DMS provider and the cloud storage provider? If all of the financial institution's vendors "encrypt," does that meet the financial institution's obligations? How far does this obligation extend - that is, does the requirement to encrypt apply to all third parties with which the dealership shares that information?

This last question is particularly important. Would this or similar requirements apply to any entity that obtains or has access to any personal data, or just if they have access to NPI? Or, does it just apply to "data processors?" What does that mean? Does it apply to entities who store the data only? Those who provide ERP services only? What about subcontractors and others who receive this information from these third parties? How does a financial institution know where to draw that line?

Dealers, like many other financial institutions, must share data with a number of third parties as part of their routine business operations: finance companies, automobile manufacturers, state taxation and registration authorities, insurance companies, and others to name a few. And, of course, each of these third parties will have its own service providers and subcontractors that

[58] Id. at 13166.

[59] It is unclear as outlined in the Notice whether this step would be required, or if it alone would be enough to comply.

handle and process the data on its behalf. Are all of these entities required to encrypt data (however that would be accomplished) as a condition of the dealership sharing that information? Is that accomplished by contract? Is a contractual provision required? If not, then what is the security benefit of requiring the dealership alone to encrypt the data? If so, then that would not only exponentially increase the cost of this requirement, it would present a practical impossibility for our members.

We understand that some of these questions would ostensibly be answered by other requirements such as contractual audit rights. The problem is that no dealership or other financial institution will be able to require, for example, a state DMV[60] or a state taxation authority (and all of its IT service providers) to encrypt data as a condition of sharing that data – much less require them to allow a third party to audit their data encryption.

Lastly, what can a financial institution do if one or more of its service providers does not or cannot meet one or more of these requirements? It may be simple to say that the financial institution should just choose another vendor, but that may not always be a viable option. Many of these systems are difficult to change, and in some cases, there may be little or no ability to change. By way of one example in the automobile industry – what if a dealer's manufacturer franchisor, or the manufacturer's captive finance company (or one of its vendors) is unable or unwilling to meet one or more of these requirements? A dealership cannot simply choose another franchisor. In the not-so-distant future, it is very likely that NPI will be transmitted from and through the automobile itself to the dealer.[61] The dealership cannot require the vehicle to be designed in any particular way and cannot choose to only allow an interface with a properly "encrypted" system.

Similar considerations apply to many of the other requirements outlined below, such as multi-factor authentication or disposal restrictions. And this is one important reason why these prescriptive requirements are impractical and of limited utility. If adopted, however, we would ask, at the least, that the Commission explain in detail exactly how far down the "chain of data custody" these types of requirements apply, and exactly what steps a financial institution must take

---

[60] As noted, dealers routinely (often as required by law) share information with state DMV's and state taxation and other authorities. Dealers not only do not have insight or ability to control their security practices, some DMVs sell the data they receive from dealers [*see, e.g.*, https://www.wptv.com/news/state/florida-dmv-sells-your-personal-information-to-private-companies-marketing-firms] Would such sales by authorized third parties be permitted, or would the financial institution need to prohibit that practice? How?

[61] For example, a customer in the course of a vehicle test drive could have the ability to provide credit application information through the in-vehicle computer system. Or the customer could extend a lease or exercise a purchase option through an interface with the vehicle. While these options largely do not exist today, there are a variety of other ways that NPI or other sensitive information generated by and through the vehicle is or could be sent to and/or accessible by the dealer.

to comply and how they can demonstrate compliance with these requirements. We would urge the Commission to make it clear that: (a) these obligations only apply to the systems directly controlled by the financial institution, and (b) that the financial institution can demonstrate compliance with these requirements by including contractual requirements and taking other reasonable steps (within the financial institution's ability to execute) to ensure that the service providers systems met the required parameters.

1. Proposed Paragraph (c)(1) - Required Access Controls.

Proposed Paragraph (c)(1) would require financial institutions to place "access controls on information systems designed to authenticate users and permit access only to authorized individuals."[62] While we agree that most financial institutions already place some type of access controls on their systems in the form of passwords or other controls, we are concerned that the scope of this requirement remains unclear. For example, the Notice cites to the Commission's consent order with Uber, where the Commission alleged that Uber "failed to implement "reasonable" access controls."[63] What are "reasonable" access controls, and how do they relate to the access controls required under this section? If what is required are "reasonable" access controls, why is this new requirement needed at all?

2. Proposed Paragraph (c)(2) - Required Data and Systems Inventory.

Proposed Paragraph (c)(2) would require financial institutions to conduct a data and systems inventory. In particular, it would require financial institutions to "identify and manage the data personnel, devices, systems, and facilities that enable [the financial institution] to achieve business purposes in accordance with their relative importance to business objectives and the [financial institution's] risk strategy."[64] While it certainly makes sense for a financial institution to understand its systems and conduct internal data assessments, this requirement is vague and

---

[62] Id. at 13166 (citing Complaint, *Uber Technologies, Inc.*, No. 152 3054 (Oct. 26, 2018).

[63] Id n. 86. In that case, the Commission alleged that Uber failed to properly monitor and control employee access to sensitive information. Is that a duty implicated under this subsection? Would that duty include the extensive steps outlined the *Uber* Complaint? If so, it is not clear from the proposed language in (c) (1). See *Uber* Complaint at 4-5 (detailing Uber's failure, to: (a) "implement reasonable access controls to safeguard data stored in the Amazon S3 Datastore;" (b) "require programs and engineers that access the Amazon S3 Datastore to use distinct access keys, instead permitting all programs and engineers to use a single AWS access key that provided full administrative privileges over all data in the Amazon S3 Datastore;" (c) "restrict access to systems based on employees' job functions;" (d) "require multi-factor authentication for individual account [and] programmatic service account access;" among other alleged failures.) found at https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf.

[64] Id. at 13166.

unclear. What exactly does this require a financial institution to do? The Notice states that this would "require a company to understand which devices and networks contain customer information, who has access to them, and how those systems are connected to each other and to external networks."[65]

First, what is the purpose of this analysis, and why is there a need to explicitly list this requirement? While it certainly makes sense to conduct a data and systems inventory, such an inventory standing alone does not provide any security for the data. Of course, the requirement does not stand alone in the Rule, but as noted above, the security benefit of this exercise seems hollow unless extended greatly, in light of the connected nature of these systems and the complexity of the data ecosystem that most financial institutions operate in. What security benefit will there be for a financial institution to conduct this type of inventory for "devices [that] contain customer information," if those devices cannot be contained or secured?

For example, a small dealership conducts this inventory and determines that personal cell phones of its employees may contain phone numbers of some of its customers – which could be NPI in some circumstances. Simply conducting this inventory does not do anything to aid in security, unless the dealership then takes steps to ensure that either the numbers are deleted and that those phones no longer can be used to call finance customers (which could cause a significant business disruption), or somehow takes steps to ensure that Apple and Samsung secure the information in those phones. The point is that this new requirement must be viewed as encompassing much more than just conducting an inventory. It also implicitly includes all steps needed to rectify any issues found when conducting such an inventory. We ask for clarification of the extent of this new duty. What steps are required to comply with this new requirement?

There are also a number of open questions about how exactly this inventory would be accomplished. Must the [newly required] CISO conduct this inventory?[66] How does a financial institution demonstrate compliance with this requirement? Must it be recorded or formalized in some way? Would a financial institution that entirely outsources its IT infrastructure to one entity be required to engage in this exercise? We ask that the Commission provide a series of examples for this and many of the other new requirements in the Notice that would allow financial institutions to understand some of the specific methods they can employ to comply with the new requirements.[67]

---

[65] Id at 13166.

[66] If so, this would increase the cost estimates outlined in Appendix A.

[67] Under the current flexible guidance, the answer to these questions is generally that they must be done as is reasonably necessary to safeguard the data. Once prescriptive requirements such as these are imposed, it becomes incumbent on the Commission to issue further guidance, or at the least, examples of compliant methods.

Lastly, it is unclear how the financial institution can comply with this inventory to the extent that it is required to do so "in accordance with the relative importance [of the personnel, devices, systems, and facilities] to business objectives and [the financial institution's] risk strategy."[68] What does this mean, and how should a financial institution view it in complying with this requirement? Does this mean that financial institutions would only be required to inventory those personnel, devices, systems and facilities that are "important?" Or does this mean that a part of the inventory is to assign a relative importance to each? How would that be determined? What is the risk strategy that this refers to? Once identified, what exactly does it mean to "manage" those items, and how would a financial institution demonstrate compliance with this requirement to manage? Does it imply proper management? And, if so, according to what principles or requirements?

This effort will be substantial and costly. The cost analysis for implementing this requirement is estimated at $16,500 in up-front costs per dealership, with an additional cost of up to $10,250 per year for the average dealership (see Appendix A.)

3. Proposed Paragraph (c)(4) - Requirement to Encrypt Data at Rest and in Transit.

Proposed paragraph (c)(4) would "generally require financial institutions to encrypt all customer information, both in transit and at rest."[69] This requirement is not styled as a "clarification," unlike several of the others. Instead, this is clearly a new requirement, and the Commission supports this requirement noting that "encryption is an appropriate and important way to protect customer information," and citing HIPAA and the FTC enforcement action against Uber.[70]

As outlined above, the scope of this requirement is unclear, as is the way that a financial institution can demonstrate compliance. We also express concerns above about the definition of "encryption." Beyond that, it is unclear exactly what "encryption at rest" means, and what is required. Does it require full-disk encryption, file system encryption, database encryption, or something else? Does it matter if the data is stored in the cloud or other remote location? Lastly, we note that IT experts we have consulted indicate that a generic requirement to encrypt at rest may provide, in many cases, illusory benefits. We express no particular opinion on the answer to these technical questions but ask that the Commission clarify as appropriate if this requirement is adopted.

---

[68] NPRM at 13166.

[69] Id.

[70] Id. at 13166, nn 92, 93.

Similar clarification is needed for the new requirement to encrypt "in transit." Does that apply to internal system data sharing, or only with outside third parties? Does it require source and endpoint authentication as well as encryption? Does a secure API structure meet this requirement?

While we agree that encryption is a good idea in theory, no evidence has been put forth that details the security benefit that this step provides. In addition, we are concerned that requiring this step for all financial institutions for all customer information may not be appropriate – especially given the cost of implementing these steps.

The cost analysis for implementing this requirement is an estimated $8,500 in up-front costs, with an additional $9,000 per year per dealership (see Appendix A.)

4. Proposed Paragraph (c)(5) - Requirement to Adopt Secure Development Practices.

Proposed Paragraph (c)(5) would require financial institutions to "adopt secure development practices for in-house developed applications utilized" for "transmitting, accessing, or storing customer information," and to develop "procedures for evaluating, assessing, or testing the security of externally developed applications they utilize to transmit, access, or store customer information."[71]

It is unclear, and no explanation is given, why special treatment is needed for in-house developed applications. While the vast majority of our members do not have the IT infrastructure or apparatus to engage in such development, it is unclear why those financial institutions that do have such capabilities must spend the resources necessary to engage in such a formal procedure.

For the majority of our members that do not have such IT in-house capability, the second requirement under (c)(5) is even more concerning. This seems to suggest that a financial institution must itself somehow evaluate, assess, and test externally developed software. How exactly is a small financial institution supposed to accomplish this requirement? The only possible way it could be done would be to hire an IT expert to accomplish these tasks. That is expensive and becomes circular – if you need an IT expert to review the security of software developed by other IT experts, how does that help? Do you need another IT expert to double-check the second one you hired?

While we understand the need to "take steps to verify that applications they use to handle customer information are secure,"[72] we can see no security benefit from requiring the financial institution itself to assess or test security. How is that done? Our members are not "white hat" hackers, and most would not know even where to begin to hire someone to conduct such testing -

[71] Id. at 13166-67.

[72] Id.

and even if they did, how would they know what to test and how? The Commission cites two enforcement cases against two large technology companies in support of this requirement.[73] However, what may be reasonable security testing and assessment requirements for a company that is among the world's largest manufacturer of routers[74] or personal computers[75] is simply not reasonable for a car dealership with no internal IT staff.

As is generally the case with the other proposed new requirements, the analysis of the costs associated with this requirement is difficult (and in this case, particularly difficult), as the scope and scale of this requirement are unclear. However, the best estimate from our IT experts is that this requirement alone would cost the average dealership $37,500 in one-time up-front costs, with an additional $9,000 per year thereafter (see Appendix A.)

This vast expense would be expended for questionable security value at best. We would suggest that it makes far more sense to continue the current requirements to conduct due diligence on service providers and ensure proper contract terms in service provider contract than it does to require sophisticated and expensive IT testing to be conducted by every financial institution in the country.

5. Proposed Paragraph (c)(6) – Required Multi-Factor Authentication.

Proposed Paragraph (c)(6) would require financial institutions to "implement multi-factor authentication for any individual accessing customer information" or "internal networks that contain customer information."[76] We have several concerns about this new requirement, and we oppose it for the reasons outlined below.

First, we think that a blanket adoption of such a requirement ignores not only the costs associated with this requirement, but also the tremendous potential business disruption it represents. This would require additional steps and seconds, if not minutes, every time any employee signed onto computer systems or accessed data. While difficult to quantify, the cumulative effect of these additional steps would be tremendous in terms of time lost, and that should not be overlooked.

---

[73] Id. at 13167 nn. 95 and 96, (citing the Complaint in FTC *v D-Link Systems, Inc.* No. 3:17-CV-00039-JD (N.D. Cal. March 20, 2017) ("D-Link"), and the FTC Complaint against *Lenovo*, FTC No. 152-3134 (January 2, 2018).)

[74] D-Link is a "manufacturer of routers, Internet-Protocol cameras, and related software and services intended for use by consumers throughout the United States." (D-Link Complaint at ¶ 6).

[75] Lenovo "is one of the world's largest manufacturers of personal computers, including desktop computers, laptops, notebooks, and tablets…." (Lenovo Complaint at ¶ 3).

[76] NPRM at 13167.

In addition, this requirement is not appropriate or necessary for all financial institutions. The Notice[77] cites to the FTC's complaint against TaxSlayer, which alleged that TaxSlayer's failure to implement dual factor authentication was unreasonable under the Rule. TaxSlayer is a tax preparation service[78] with perhaps the most sensitive financial information available, that is specifically designed to routinely allow remote access to its systems to millions of consumers. Whether it is reasonable to adopt dual-factor authentication in a system with particularly sensitive information that is widely accessed by non-employees and others is simply not relevant to most financial institutions, and this is a good example of a misguided effort to apply a specific fact pattern to all financial institutions, regardless of size or circumstance. Such tools may not make sense or add any material security benefit in a situation where third parties do not routinely access data or systems, and the data at issue is not as highly sensitive.

In a dealership, for example, salespeople or other dealership personnel may need to have access to systems or databases that show whether a customer leased or financed a vehicle. That information is likely to be protected under the Rule. However, an expensive security requirement such as this for those employees to access that information will add not only cost, but time and effort every time they log into a system, while providing little to no additional security protection for the consumer.

In addition, we are concerned about several of the positions outlined in the Notice with respect to the factors allowed or promoted. First, the Notice specifically lists "biometric characteristics" as an example of an "inherence factor" that could be used as the one of the two types of authentication factors under this new requirement.[79] But biometric data is highly sensitive, indeed *far more sensitive* than some of the NPI that financial institutions like dealerships maintain, because it cannot be changed or amended if breached. State laws have been passed specifically to protect biometric data[80] and several of the recent broad privacy regimes specifically list biometric data as highly sensitive.[81] We disagree with the imposition of a federal requirement

---

[77] Id.

[78] TaxSlayer "advertises, offers for sale, sells, and distributes products and services to consumers, including TaxSlayer Online, a tax return preparation and electronic filing software and service." (FTC Complaint against TaxSlayer at ¶ 3, found at https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_complaint.pdf).

[79] NPRM at 13164.

[80] The Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. (BIPA), found at http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004. (see also Tex. Bus. & Comm Code Ann § 503.001; Wash. Rev. Code 19.375.)

[81] See CCPA, 1798.140 (b) (defining "Biometric information" as "an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual

that could be seen as promoting the use of biometric data, and any financial institution that began to collect biometric data like retina scans or fingerprints(!) to comply with this requirement would be creating tremendous *additional* unnecessary privacy and security risks – well beyond any security benefit achieved by the dual factor protections. Employees of financial institutions should not be required to sacrifice the sanctity of their own personal, inherent, and non-changeable information of the most sensitive nature in order to be permitted to "access customer information" under the Rule. We strongly urge the Commission to delete this category as one of the permissible factors allowed under this requirement.

At the same time, the Notice rejects the ability to use text messages as a permissible second factor under this requirement.[82] We do not believe this is reasonable. First, it prohibits the most commonly used, cost-effective, and user-friendly choice for second factor authentication.[83] Second, it underestimates the benefits of such a system and overestimates the risks. We do not believe that rejecting its use will materially aid in the security of financial institutions' systems and, at the least, this issue requires further analysis before being rejected as an option.

Lastly, we note that the Notice states that an institution "may adopt" a reasonably equivalent method, "with the written permission of the CISO."[84] We object to this standard for allowing a reasonable alternative to dual factor authentication. As outlined herein, we believe that

---

identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."); see also Article 4, EU General Data Protection Regulation (defining biometric information as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data.")

[82] Id. at 13164, n. 74, (noting that "the proposed amendment deviates from the language of the Cybersecurity Regulations in that it does not include text messages as an example of a possession factor.") In addition to the fact that we do not believe that such a restriction is warranted or necessary, this footnote raises the question of how the Commission can state that financial institutions "ha[ve] considerable flexibility in how to implement each factor" (Id. at 13166), at the same time as implicitly prohibiting the use of text messages as a possession factor simply because text messages are not included as an example of such a factor? Does this mean that any method not listed as an example is impermissible? How does that allow for "considerable flexibility?"

[83] Indeed, many federal government agencies (such as the Department of Homeland Security in connection with its "Trusted Traveler Program, and elsewhere) use text messages as the second factor for sensitive and secure functions. See, e.g., https://www.login.gov/help/privacy-and-security/how-does-logingov-protect-my-data/.

[84] NPRM at 13167.

most dealers and smaller financial institutions will need to outsource the CISO function to a third party. This standard, as articulated (here and in other similar provisions in the Notice), would require decisions such as these, that affect critical business practices at a financial institution, to be dictated by a third party with no stake in the business outcome. This grant of authority to a third party, whose primary motives are different from (and in some cases at odds with[85]) the financial institution creates a real potential for a conflict of interest, and we do not believe that any non-employee of a financial institution should be granted such authority over the operations of the financial institution.

The cost analysis of this new requirement reflects an additional one-time, up-front cost ranging from $33,750, with an additional annual cost of $18,500 per year, for the average dealership. (See Appx. A.)

6. Proposed Paragraph (c)(7) – Requirement to Include Audit Trails.

Proposed Paragraph (c)(7) would require financial institutions to "include[86] audit trails designed to detect and respond to security events." The notice defines "audit trails" as "chronological logs that show who has accessed an information system and what activities the user engaged in during a given period."

This required use of "audit trails" "to detect and respond to security events" is overbroad and unclear. First, this would include not just material breaches but, given the broad definition of "security event" included in the Notice, any unauthorized access to customer information. The scope of this requirement is potentially very broad, with little relation to data security. Second, it is unclear how such trails would be used to "detect and respond," but it seems at the least to be creating another new obligation not just to "include" audit trails, but also to actively monitor these trails, and this obligation will have a significant cost. Must a financial institution engage yet another employee to monitor these "trails" to ensure detection or is this something that can be fully automated?[87]

Is there a standard by which a financial institution can ensure that they are monitored properly? How can or should a financial institution properly respond if it detects unauthorized

[85] For example, an outsourced CISO who must approve such steps would have a strong interest in protecting itself (not the financial institution) from liability or responsibility, as well as a financial interest in selling more IT services and products to the financial institution. It would therefore be highly incentivized to reject any alternative approaches regardless of business need, efficiency, or cost.

[86] There is a threshold question of "included in what?" How does an "information system" under the Rule "include" such trails? Does this requirement apply to all "information systems?" How is that defined? Can this requirement be met by including one audit trail that documents all system access, or must each system contain its own?

[87] Outside IT consultants have informed us that in many cases, audit log monitoring such as outlined in the Notice is an issue that is difficult, if not impossible to automate.

access via this new monitoring duty? Will this response need to be coordinated and monitored by the new CISO? If so, that would add additional costs to the estimates outlined above and in Appendix A.

Lastly, the requirement to create such audit trails would be another of several requirements outlined in the Notice that would dictate the creation of documents or records that could theoretically be used to aid in securing data but will also certainly be demanded after the fact by those seeking to place blame for any alleged security incident. It should be recognized that a requirement to create an extensive "paper trail" of any kind will lead to lawsuit abuses, because it will become a simple matter to demand access to this data in connection with a lawsuit related to an alleged "security event," regardless of the merits of any such claims. Such demands will be expensive to comply with, which will increase the ability of third parties to extract settlements. These records could also be easily distorted and second-guessed by third parties seeking to extract compensation for an alleged security event. This and the other requirements in the Notice to create such records will create a fertile ground for abuse.

Liability exposure aside, the cost analysis of this new requirement reflects an average one-time up-front cost of $30,000 per dealership, with an additional $18,000 per year for the average dealership. (See Appx. A.)

7. Proposed Paragraph (c)(8) – Requirement to Develop Secure Disposal Procedures.

Proposed Paragraph (c)(8) would require financial institutions to "develop procedures for the secure disposal of customer information…that is no longer necessary for their business operations or other legitimate business purposes."[88]

First, we strongly object to this new requirement to the extent it is seeking to create a new duty for financial institutions to dispose of customer information unless "necessary for business operations" or "no longer necessary."[89] We do not believe that the Rule contains any authority to require financial institutions to delete any information, and we object to this requirement to the extent it seeks to impose such a broad and drastic requirement. We agree that it can be good practice to delete information that is no longer necessary, but any such decision is voluntary and, as long as the data continues to be protected, such retention should not be subject to the Rule.

These concerns are especially acute given the questions in the Notice as to whether financial institutions should be required: (a) "to affirmatively demonstrate a current need for customer information that is retained," or (b) "to develop procedures to limit the collection of customer information that is not necessary for business operation or other legitimate business

[88] NPRM at 13167.

[89] Id.

purposes."[90] Such requirements would be nothing short of a new privacy regime that would have business implications well beyond the scope of the Rule and unconnected to data security. Such suggestions are particularly untimely given the current federal privacy debate, and unwarranted given the applicability of the CCPA[91] and other privacy regimes that would place certain limited restrictions on the collection of certain types of data.

Second, while properly disposing of customer information is important, we believe that a requirement to "develop [such] procedures" is overly complicated for most financial institutions, and unclear. The FTC Disposal Rule,[92] which applies to consumer reports or information derived from consumer reports, provides a much clearer and more effective standard. That rule requires disposal practices that are reasonable and appropriate, including "burning, pulverizing, or shredding" papers or physical media containing protected information and "destroying or erasing electronic files or media" containing protected information. Indeed, the Commission has already noted that "financial institutions that are subject to both the Disposal Rule and the [Safeguards] Rule should incorporate practices dealing with the proper disposal of consumer information into the information security program that the Safeguards Rule requires."[93] There is no indication that this current guidance does not work well or that it creates any security risks that would be solved by requiring financial institutions to create new procedures.

The cost analysis of this new requirement reflects an average one-time up-front cost of $30,000 per dealership, with an additional $10,800 per year in added cost for the average dealership. (See Appx. A.).

8. Proposed Paragraph (c)(9) – Required Adoption of Procedures for "Change Management."

Proposed Paragraph (c)(9) would require financial institutions to "adopt procedures for change management," which "govern the addition, removal, or modification of elements of an information system."[94] This means that financial institutions "would need to develop procedures

---

[90] There is simply no reason why a financial institution should be limited in their collection or retention of data in any way that is different from any non-GLB entity. We do not question the wisdom of such restrictions – if applied universally. But there is no reason to impose such restrictions solely on GLB financial institutions, and we do not believe there is any authority under the Rule to seek to do so.

[91] CCPA creates an opt-out requirement (GDPR is an opt-in system), but they are both rules of general applicability, and neither go so far as to say that any entity is prohibited from obtaining any class of information from any individual if such rights are provided.

[92] 16 CFR Part 682" Disposal of Consumer Report Information and Records."

[93] See https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how (citing ftc.gov/privacy/privacyinitiatives/safeguards.html)

[94] NPRM at 13167.

to assess the security of devices, networks, and other items to be added to their information system or the effect of removing such items or otherwise modifying the information system."[95]

While such considerations would seem to be a sensible part of business decisions, the scope of such procedures is unclear. In addition, it is not reasonable to require all financial institutions – including those that have not had any material change for some time, and do not anticipate any such material change to their internal systems in the future[96] – to take the time, effort, and expense to develop a procedure for taking such a common-sense approach. We believe this should be applied to financial institutions for which it could be applicable, and not to all entities regardless of circumstances.

The cost analysis of this new requirement reflects an average one-time up-front cost of $30,000 per dealership, with an additional $2,000 per year for the average dealership. (See Appx. A.)

9. Proposed Paragraph (c)(10) – Required Unauthorized Activity Monitoring.

Proposed Paragraph (c)(10) would require financial institutions to "implement policies and procedures designed "to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users."[97] This would create another new requirement to monitor employees and other authorized users and their activities. Again, the implications of this new requirement are extensive. This means that financial institutions must not only establish and maintain appropriate access levels and activities for all authorized users, they need to continually monitor all authorized user use. This has tremendous implications for employee policies and privacy and will not be something that can be easily automated. Again, this means yet more new employees or third-party IT consultants who will be making important business and operational decisions for the financial institution.

They will have to monitor and adjudicate unique circumstances, such as "transferring large amounts of data or accessing information for which the user has no legitimate use." There may be legitimate reasons for such activity, but it will need to be determined on a case by case basis. Again, as with many of these requirements, we do not take issue with the notion that there is merit to this step, and that many financial institutions will implement some version of this control. However, by making this an explicit, stand-alone requirement, the Commission is enshrining costs and efforts that will be extensive and will likely not be needed in all circumstances.

---

[95] Id.

[96] This does not mean that they do not anticipate adapting their programs to keep up with changes in data security, although that does not appear to be the focus of this new requirement.

[97] NPRM at 13168.

The cost analysis of this new requirement reflects an average one-time up-front cost of $20,000 per dealership, with an additional $29,000 per year in added cost for the average dealership (see Appendix A.)

vi. Proposed Paragraph (d) – Required Penetration Testing and Vulnerability Assessments.

Proposed paragraph (d) would require financial institutions to include in their regular testing of their safeguards, either "continuous monitoring" or "periodic penetration testing and vulnerability assessments."[98] Continuous monitoring is any system that allows real-time, ongoing monitoring of an information system's security, including monitoring for security threats, misconfigured systems, and other vulnerabilities.

The cost analysis of this new requirement reflects an average one-time up-front cost of $20,000 per dealership, with an additional $29,000 per year in added cost for the average dealership for ongoing monitoring (see Appendix A.)

vii. Proposed Paragraph (e) – Required Employee Training and Security Updates.

Proposed Paragraph (e) contains a series of new training and security requirements. We address each in turn:

First, it would require financial institutions to ensure that "personnel are able to enact the information security program"[99] through various forms of training, including "security awareness training that is updated to reflect risks identified by the risk assessment."[100] This training requirement would apply to "all personnel that have the ability to handle, access, or dispose of customer information," and would "be designed to inform personnel of the risks to customer information and the financial institution's policies and procedures to minimize this risk."[101] This suggests that the training would need to be specifically tailored to the individual financial institution, which increases the cost of such training significantly, and in our view, unnecessarily. Training is essential but general security awareness is more than enough for 99% of security incidents. Consequently, the cost of requiring a specific tailoring of the training to any specific policy or procedure needs to be weighed against its limited benefit.

---

[98] Id.

[99] Id.

[100] Id at 13176.

[101] Id.

This training could be performed by an outside service provider. Most of our members do not have the internal capability to provide such training, so they would be required to engage a third party.

Second, financial institutions would be required to "utilize qualified information security personnel...to manage [their] information security risks and to perform or oversee the information security program."[102] This is very unclear and needs to be clarified. The Notice states that this "is intended to ensure that information security personnel used by financial institutions are qualified and that sufficient personnel are used."[103] What does this mean? What constitutes security personnel? What if a financial institution did not currently have enough "qualified" personnel to oversee their program? Would they be required to hire yet another highly paid IT professional? Is this referring to the CISO? It appears that it may be in addition to "senior cybersecurity personnel."[104] In any event, what does "qualified" mean, and how does a financial institution ensure this qualification?

Again, this is unclear, but assuming that this means that dealerships would need to hire one or more additional IT professionals, the estimated cost for this requirement is anywhere from $75,000 to more than to $100,000 per year depending on the part of the country and the nature, number and qualifications of these new employees or consultants. These numbers are not included in the overall cost estimates below because this is unclear and difficult to estimate, but it would clearly add significant costs in addition to that outlined below, if, as it appears, it requires new IT personnel.

Third, proposed Paragraph (e) contains a requirement to "provide information security personnel with security updates and training sufficient to address relevant security risks."[105] This appears to require ongoing training, as it seems to require a financial institution to identify the risks that are relevant to its operation, and procure and provide that specific type of training to the new "information security personnel." This would add significantly to the costs required to meet this new training requirement.

Lastly, proposed Paragraph (e) would require all financial institutions to "verify that key information security personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures."[106] The examples of compliance with this requirement demonstrate

---

[102] Id. at 13168.

[103] Id.

[104] Id. at 13169.

[105] Id at 13168.

[106] Id.

its inapplicability to most smaller financial institutions -- these include "incentives for continuing education" and "annual assessments of key personnel's knowledge of threats related to their information system."[107] Who exactly is going to perform these assessments? The financial institution itself, or does it need to hire another third-party service provider to test the third-party service provider it hired to act as qualified security personnel?

The cost analysis of this training requirement reflects an average one-time up-front cost of $2,100 per dealership, with an additional $5,500 per year in added cost for the average dealership - based on generic, online cybersecurity awareness training. If, as the Notice seems to suggest, financial institutions would be required to develop and implement custom training for their employees based on that financial institution's "policies and procedures," and "relevant security risks" then the estimated cost increases to an average one-time up-front cost of $15,000 per dealership, with an additional $15,000 per year for the average dealership. (See Appx. A.)

We strongly support training and taking reasonable steps to ensure that competent personnel are addressing security issues. However, these exacting requirements are not necessary or appropriate for all financial institutions and they would, therefore, impose unnecessary costs. If these new requirements are imposed, it will cause disproportionate harm to smaller financial institutions who do not have the in-house capability to address these issues. Rather, they will be forced to engage expensive third-party service providers to oversee their existing expensive IT providers.

viii. Proposed Paragraph (f) – Required Periodic Assessment of Service Providers.

Proposed Paragraph (f) would "add a requirement that financial institutions periodically assess service providers 'based on the risk they present and the continued adequacy of their safeguards.'"[108] This is "designed to require financial institutions to monitor their service providers on an ongoing basis to ensure they are maintaining adequate safeguards…."[109]

This new requirement would be difficult and expensive. Among even our largest members, given the scope and complexity of the data ecosystem, this would be a very time-consuming effort and likely require the addition of a new, highly compensated, full-time equivalent employee. It is also unclear how financial institutions, particularly smaller financial institutions, could accomplish this requirement. What are the adequate safeguards that the service provider must employ? Are

[107] Id at 13168-69.

[108] Id at 13169.

[109] Id.

they exactly the same as those required under the Rule?[110] How would a dealership or other small financial institution be able to make and confirm that those steps are being taken? Is it enough to place such requirements in the service provider contract, and then periodically receive confirmation from the service provider that those requirements are being met?

Concerns have also been related to us that it would, in many cases, not be technically possible for a financial institution (of any size) to engage in such a risk assessment because the level of granularity of access needed to conduct such an assessment is simply not available (either because of limitations in the service providers underlying architecture, or because they will not agree to the level of specificity needed).

Our members understand the need to continually monitor service providers but are concerned that this requirement will be too expensive or difficult to be feasible. We would encourage the Commission to allow financial institutions to meet this requirement via contractual commitment and agreement, or other reasonably available means. We agree that service providers need to be monitored, and, as noted above, we would ask the Commission to consider identifying tools that can be provided to financial institutions to allow them to adequately and realistically monitor their service providers and hold them to account if they do not meet their contractual commitments.

The cost assessment estimates an additional $14,250 in one-time costs, with an additional $11,250 per year in additional costs for the average dealer.

ix. Proposed Paragraph (h) –Required Incident Response Plan.

The Notice also contains a new explicit requirement for financial institutions to adopt a seven-part "incident response plan."[111] This raises several important concerns, and NADA is opposed to the inclusion of this new requirement.

As an initial matter, the term "incident response plan" should be defined. We are not aware of any widely-recognized definition, but it can generally be described as a plan to prepare for a "cyber event" and to be able to respond to a range of events if they occur. Both NIST and SANS are widely cited sources for Incident Response Plans and a review of their respective incident response checklists shows how complicated they can be.[112] In short, these plans require an entity to take steps to mitigate the harm to the entity after a cyber event has been identified as having occurred, and to coordinate and communicate about the event as appropriate. While these may be

[110] See discussion above about exponential increases in complexity and cost if these requirements are imposed throughout data ecosystem.

[111] NPRM at 13160.

[112] See https://www.sans.org/media/score/checklists/APT-IncidentHandling-Checklist.pdf and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

sensible and even laudable steps for a financial institution or other entity to prepare for, requiring such a plan is not appropriate under the Rule.

First, we believe this requirement is outside the scope of the Rule and the statutory mandate under GLB because it is not a step taken to protect the security or confidentiality of customers' NPI nor does it prevent data breaches or other "cyber events." Such plans address a financial institution's *response* to a detected "event," which may be prudent, but it is simply not part of establishing standards to safeguard data and therefore not an appropriate requirement under the GLB statutory mandate – which is limited to the establishment of appropriate standards relating to administrative, technical and physical safeguards to: (a) insure the security and confidentiality of customer information, (b) protect against anticipated threats or hazards to the security or integrity of such records, or (c) to protect against unauthorized access to or use of such records. [113]

In addition, the Rule defines "Information Security Program" as "*the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information*." That, appropriately, addresses the protection and "safeguarding" of sensitive data, but does not include or address in any way, steps that may be taken in the aftermath of a "cybersecurity event." Again, while it may be laudable and sensible for a company to have a plan in place to react *after* a "cybersecurity event,"[114] any after-action plan cannot by definition be related to any standard to safeguard data. Rules about what happens after the "horse gets out of the barn" (while useful) are simply not related to the steps required to keep the horse in the barn in the first place.

Second, even if an incident response plan were appropriate to require under the Rule, what would this plan need to include and why? In other words, what other steps might financial institutions be "required" to consider or adopt as part of this plan – either explicitly in the future, or implicitly under a "reasonableness" standard? First, must this incident response plan address all types of security incidents, or only those that could affect NPI? Is that true for all financial institutions – why or why not? Must a financial institution include a plan to compensate

---

[113] 15 USC 6801 **(**a) Privacy obligation policy: It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to *protect the security and confidentiality of those customers' nonpublic personal information*.
(b) Financial institutions safeguards: In furtherance of the policy in subsection (a), each agency or authority described in section 6805(a) of this title, other than the Bureau of Consumer Financial Protection, *shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards-(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. (emphasis added).*

[114] NPRM at 13161.

individuals affected by a cybersecurity event, for example by providing "credit monitoring" or other prophylactic protections for affected consumers? Is that true for all cybersecurity events or only those resulting in a significant risk of identity theft? Must financial institutions address liability issues in their contracts with service providers or insurance companies? Must this plan include a disaster recovery component?[115] A public relations or legal strategy? Many of these issues are often standard or recommended components of an incident response plan,[116] and it is generally a good practice for businesses to adopt such measures to protect business interests. Such issues are outside the purview of the Rule. In addition, it is unclear which, if any, of these must be part of any such plan, or how a financial institution would determine which, if any, are required. This lack of clarity fails to provide financial institutions with the certainty they need to ensure that they can meet any such prescriptive new requirement. Of course, the costs of enacting (and following through with) such a plan would be affected greatly by the required scope of that plan.

Third, while the Notice states that this change "is not intended to create any independent reporting or notification requirements, nor to conflict with any such requirements to which financial institutions are already subject,"[117] it is unclear how that would work in practice. Customer notice is a standard component of most incident response plans. Indeed, identifying and notifying affected consumers of the cybersecurity event is the central purpose of most plans. Consumer notice is provided, in part, to ensure compliance with state data breach laws. By imposing the requirement to have an incident response plan, this notice required is also being imposed *de facto.* We do not believe that any new federal requirement for financial institutions to notify affected consumers - or the Commission[118] - about "cybersecurity events" is appropriate, not only because it is outside the GLB statutory mandate, but also because consumer notice is already governed and required by state law.

Each of the 50 states, Guam, Puerto Rico and the Virgin Islands have all enacted data breach statutes.[119] These state data breach laws are, at heart, basically consumer notification

---

[115] "Disaster Recovery Planning" - Planning to ensure the timely recovery of information technology assets and services following a catastrophe, such as fire, flood or hardware failure." Gartner IT Glossary, found here https://www.gartner.com/it-glossary/drp-disaster-recovery-planning/

[116] See e.g. the SANS checklist at n. 17.

[117] NPRM at 13169.

[118] Id. (asking "whether the proposed amendment should require that financial institutions report security events to the Commission.")

[119] See http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

regimes. While the Commission has repeatedly sought a national data breach law,[120] including a duty to notify consumers,[121] such a federal statute does not yet exist, and we do not believe it is appropriate to indirectly impose federal data breach duties that Congress has not yet seen fit to empower the Commission to do, via a rulemaking under the Safeguards Rule.

Fourth, an incident response plan deals primarily with steps an entity may take to mitigate the impact of certain types of cybersecurity incidents if they occurred, but only in certain circumstances. It may not be viable or needed in some instances, many of which likely will not implicate any NPI or any harm or potential harm to consumers. Indeed, the "Commission agrees that "the current Rule already requires *many* [but presumably not all] financial institutions to develop an incident response plan."[122] We believe that because incident response plans vary so widely in scope, need, and applicability, it is not appropriate to impose an incident response plan requirement on all financial institutions in all circumstances.

Lastly, incident response plans generally implicate not only consumer notice, but also steps to mitigate business harm to the entity suffering the cybersecurity incident. For example, most incident response plans will address or at least consider disaster recovery planning (discussed *infra),* steps to limit legal liability, public affairs and press releases and notices, service provider indemnification, insurance issues, business continuity concerns, and other administrative and practical steps entities need to take in the wake of a cybersecurity incident. Again, it may be good business practice, but it is unclear how requiring financial institutions to address issues relating to mitigating damages for the financial institution itself and its business operations is related to ensuring that sensitive consumer data is safeguarded against a breach. We do not believe that such a blanket requirement should be imposed under the Rule.

The cost assessment estimates an additional $16,000 in one-time, up-front costs, with an additional $6,625 per year for the average dealership to comply with this requirement. (See Appx. A)

---

[120] See, e.g., https://news.bloomberglaw.com/privacy-and-data-security/ftc-commissioner-calls-for-national-data-breach-law-corrected; https://www.ftc.gov/news-events/blogs/business-blog/2018/11/ftcs-comment-future-privacy, and; https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf (at 20) (stating that "[d]ata security concerns are an important part of the privacy debate and, in light of the issues described above, the FTC continues its longstanding call that Congress consider enacting legislation that clarifies the FTC's authority and the rules relating to data security and breach notification.")

[121] The very fact that the Commission has sought statutory authority for a national data breach notification requirement demonstrates that the Commission does not believe that such authority currently exists.

[122] NPRM at 13160.

For these reasons, we would urge the Commission to reject any requirement to adopt an incident response plan as part of a financial institution's information security program. For similar reasons, we oppose any requirements in the "proposed amendment [that would] require that financial institutions report security events to the Commission."[123]

x. Proposed Paragraph (i) –Required Written CISO Report.

Proposed Paragraph (i) would require the newly created CISO to "report in writing, at least annually, to [the financial institution's] board of directors or equivalent governing body" regarding the following information: 1. The overall status of the information security program and financial institution's compliance with the Safeguards Rule; and 2. material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program."[124]

First, this required annual report would be very expensive. As noted above, we believe that most of our members would need to outsource the CISO function, at tremendous cost. Requiring this highly compensated consultant to draft such an extensive report each year, regardless of any change or activity warranting such a report will be very costly. The cost assessment for this report alone estimates an additional $9,000 in one-time costs, with an additional $9,000 per year in additional costs for the average dealership. (See Appx. A).

Second, what is the purpose of this written report and its submission to the board of directors or other governing body? It is ostensibly to "ensure that the governing body… is engaged with and informed about the state of the … information security program," and to "create accountability for the CISO" with the board.[125] However, a consequence of this requirement is that it would create unnecessary liability exposure for the board/leadership of the entity.[126] We

[123] Id. at 13169.

[124] Id. at 13170.

[125] Id.

[126] Especially if the Rule were to "require the Board or equivalent body to certify compliance with the Rule." Id. at 13170. We object to the inclusion of any such requirement. As noted, our members do not generally have Boards, and it is unrealistic and would be overly burdensome for the business leaders of a dealership to "certify whether the entity meets the complicated demands of this Rule, or whether the highly-compensated outside IT professional they have been required to engage has properly addressed the Rule's requirements. Indeed, it is difficult to see how all but the most sophisticated entities could so certify – and then, only with *additional* professional assistance.

object to this requirement, and to any requirement that the board should be required to "certify" compliance with the Rule.[127]

Most of our members do not have a board of directors or equivalent governing body. Our members are largely run by individuals who have franchise agreements with automobile manufacturers. While dealership leaders should be aware of data security measures, and indeed, should be encouraged to understand and promote these efforts, they are generally not data security experts. The entire reason they outsource these functions in the first place is because specialized IT is not their expertise. While many of our members will themselves require such accountability from the CISO they are required to engage, requiring this expensive report to be drafted for the leadership of most of our members on an annual basis will create a cost burden that would not be outweighed by any significant benefit. It will not only be expensive, it is unlikely to promote understanding or engagement. Instead, it is more likely to be filled with platitudes and/or efforts to "upsell" the dealership on additional CISO services. Most managers of most businesses are not IT experts and requiring an expensive annual report will not transform them into experts.

III. The Cost to Implement the New Requirements Would be Prohibitive – Especially for Small Financial Institutions.

As outlined herein, each of the new requirements has an attendant cost that is, in many cases significant and in some cases prohibitive. In summary, the analysis conducted on our behalf estimates that the total initial cost to the average dealership to comply with the new requirements outlined in the Notice is $293,975 in one-time, up-front costs, with $276,925 in additional costs each year. We conservatively estimate the total cost for all U.S. dealers to implement the new requirements at more than $2.2 billion in up-front costs, with more than $2.1 billion in additional costs each year in ongoing compliance costs.[128] These figures are likely to be higher on a per store basis for small dealers and other small financial institutions.

Of course, automobile dealers are just a small percentage of the financial institutions covered under the Rule. We cannot estimate with any certainty the total cost to all U.S. financial institutions because the total number of financial institutions is unclear, but even using a very conservative figure of 10X[129] for the total cost to all financial institutions resulting from the new

---

[127] Id.

[128] This is not simply the estimated costs multiplied by the total number of U.S. dealers, but a much smaller number that seeks to establish a conservative overall estimate by accounting for potential economies of scale for larger dealers, as well as for the possibility that many of these costs will not be new for many dealers. See Appendix A for details.

[129] In other words, we are not certain of the total number of financial institutions subject to the Rule, nor how many of those entities currently meet all of the requirements outlined herein. We believe that franchised dealers make up only small percentage of affected entities. Nevertheless, this overall cost

requirements results in a total up front estimated cost to implement the new requirements of more than $22 billion, with more than $21 billion in added costs each year.

This only estimates the direct costs to financial institutions, but those direct costs may pale in comparison with the indirect costs of these requirements. If, as it appears, these requirements would need to be imposed not only on financial institutions directly, but on each of the third parties service providers and "authorized users," that are part of the financial institutions' data ecosystems, these costs will multiply exponentially.

Of course, a significant portion of these costs will ultimately be borne by the consumer.

IV. Compliance with These Requirements Should Provide Safe Harbor Protection.

As outlined herein, we do not believe that the Commission should adopt these new requirements, but if it does decide to adopt one or more of them, we would urge it to adopt the changes, not as prescriptive requirements, but as a safe harbor that financial institutions could utilize if they complied with the new requirements. In other words, we would urge the Commission to continue to allow financial institutions to meet the requirements under the Rule by adopting reasonable steps to protect customer information but clarify that a financial institution that met the new proposals would be provided a safe harbor for compliance with those portions of the Rule. There are similar safe harbor analogs in other FTC regulations,[130] and those safe harbors have been effective at promoting and incentivizing behavioral change, without losing the flexibility that is crucial to ensuring compliance for a wide swath of entities with vastly different circumstances and capabilities.

V. Small Business Exemption / Size Limitation.

Proposed Section 314.6 would exempt financial institutions that "maintain customer information concerning fewer than five thousand customers"[131] from certain of the newly proposed requirements in the Notice. We agree that smaller financial institutions should be exempted from these requirements as it will be prohibitively expensive and practically impossible for many of these institutions to comply with these requirements. However, the limit as proposed would be

---

estimate reflects what we believe to be a very conservative estimate of 10 times the number of franchised automobile dealers in the U.S. (16,735).

[130] For example, the FTC provides a "model privacy form that financial institutions may rely on as a safe harbor to provide disclosures under the privacy rules." See Appx. A to Part 313, (1)(b), and https://www.ftc.gov/sites/default/files/attachments/press-releases/federal-regulators-issue-final-model-privacy-notice-form/privacymodelform_rule.pdf
There is also an FTC safe harbor for inadvertent mistakes that violate the Telemarketing Sales Rule (see https://www.ftc.gov/tips-advice/business-center/guidance/qa-telemarketers-sellers-about-dnc-provisions-tsr); as well as a COPPA safe harbor program (see https://www.ftc.gov/safe-harbor-program)

[131] Proposed 16 CFR 314.6 (see id. at 13170).

far too low. Indeed, we note that the recently passed California Consumer Privacy Act adopts an applicability threshold that is *ten times* higher -- fifty thousand consumers.[132] However, the extensive concerns we have detailed throughout these comments are not confined to our members that maintain fewer than fifty thousand consumer records. Accordingly, we urge the Commission to exempt financial institutions that maintain customer information on fewer than a minimum of one hundred thousand consumers,[133] and we would urge the Commission to apply the exemption to each of the new requirements in the Notice.

Moreover, because, as noted above, dealers obtain information from various constituencies, but only a small percentage of that information is "customer information," we believe that financial institutions such as dealers that take steps – consistent with their records retention requirements[134] – to limit the nature of the information they maintain about customers to exclude any portion of that information that makes it subject to the Rule, should also qualify for this exemption. In other words, a dealership that has 200,000 records of service or parts customers and 120,000 records containing customer information would be subject to the requirements. However, if that same dealership took steps to delete those portions of the 120,000 records that contain NPI,[135] it should also be exempt from the requirements.

VI. If New Minimum Requirements Are Imposed, the Timeframe for Implementation Must Be Extended Significantly.

As outlined above, the new requirements in the Notice would impose a significant and difficult new set of obligations for many financial institutions. These requirements would not only require technical changes of varying degrees of difficulty, and process and policy changes that will take significant time, it will require hiring new staff and vetting and engaging third party IT service providers. That new staff will then need to be educated and tasked with adopting all of these new requirements. That will be expensive and will take significant time.

Our members are concerned that the technical changes are likely to be much more extensive and time-consuming than envisioned in the Notice. For example, as noted above, the ERP providers for dealerships are called DMS providers. The DMS manages the basic business functions of the dealership like accounting and human resources, as well as specialized dealership

---

[132] See Cal. Civ. Code § 1798.140 (C)(1)(B)).

[133] In this connection, it is important to note that unlike the CCPA, exempted financial institutions would still be subject to the extensive range of other requirements under the Rule.

[134] See, e.g., Reg B, 12 CFR § 202.12.

[135] For example, as outlined in the example above, if they deleted all finance or lease identifiers, and any other sensitive financial information obtained on the credit application, but retained their name, phone number, address, and VIN of the vehicle they own.

functions such as sales, finance, service, and parts. It also manages the critical electronic interface dealers have with their manufacturer (to order and pay for cars and parts, conduct warranty repairs, manage recalls, etc.) The DMS market is dominated by two major companies,[136] which together control over 75% of the U.S. DMS market. This is relevant to the Notice because dealerships often have very few functional choices for a DMS provider, and while we would hope that, if adopted, these companies will be functionally able to comply with the proposed new security requirements, that is unclear at this point. There are indications that one or more of these companies (or other similar companies that dealers rely on to provide technology services) operate on older or unique architectures that could have difficulty with some of the requirements, like encryption. If, for whatever reason, one or more vital IT vendors do not or cannot (for technical or other reasons) meet these requirements in a timely fashion, dealers will have little choice and little ability to either require those changes or change providers. As a result, we would ask that if the requirements in the Notice are implemented, that the Commission provide a significant period of time for our members, and their critical technology providers, to take the steps necessary to meet the requirements, or if necessary, for our members to switch providers.

If the proposed new requirements are adopted, in whole or in part, we would ask the Commission to allow a significant period of time for financial institutions to comply. Without knowing specifics at this time, we would ask for at least one year from the time that these requirements are finalized, with an additional year allotted to allow for the necessary revisions of service provider and other contracts. We would also ask for an explicit acknowledgement that financial institutions like dealers whose vendors are unable to meet the technical demands in that timeframe can themselves comply with the more technical requirements by demonstrating that they are using reasonable alternative means to protect the data, while their vendors work to meet the requirements.

VII. The Commission Should Consider the Net Additional Security Benefit of Each of the New Proposed Requirements.

As outlined above, the Notice includes a litany of new and expanded explicit requirements. Let us assume for a moment that each of these new requirements does provide some measure of additional security protection. That should not be the sole determining factor whether to impose this entire "wish list" of new requirements on all financial institutions. The next step in the inquiry – and one we would urge the Commission to take here – would be to analyze the net additional security benefit of each proposal. In other words, if one or two of the steps outlined herein provided 95% of the total possible security protection at a cost of $X, while all of the steps together provided 97% of that protection at a cost of $10X, there is a real question whether it makes sense to impose those significant additional costs on financial institutions (and ultimately consumers).

By way of one theoretical example, if a financial institution successfully and effectively encrypted its data in all circumstances, both at rest and in transit, how would that affect the

[136] They are CDK Global (www.cdkglobal.com) and Reynolds and Reynolds (www.reyrey.com).

additional net security benefit of a requirement to draft and adopt a seven-part incident response plan? In other words, even if each of those requirements – standing alone – provided some material safeguarding benefit, they do not stand alone as outlined herein, and any benefit is reduced dramatically as each of the additional duty is added to the list of requirements.

We urge the Commission to engage in this type of analysis and prioritize those steps that truly make sense for all financial institutions and provide the most security benefit for consumers relative to their cost. We believe that such an analysis would, at the least, result in a much more limited universe of "required" steps for all financial institutions.

VIII. Conclusion.

Our members are committed to protecting the information they obtain from their customers. Trust is critically important, and dealerships will continue to protect the data they have. However, flexibility to adapt and protect as reasonable is critical to ensuring that financial institutions of all kinds and sizes can adequately address these issues. A one-size-fits-all approach is not only unnecessary, we are concerned that it could be counterproductive and, in many ways, unachievable.

In sum, we are opposed to these new requirements because most will add significant additional costs and other burdens for financial institution, especially smaller financial institutions. We do not believe that these additional burdens are offset by demonstrated material improvement to data security at financial institutions. These requirements have largely not been proven to be necessary or effective, and they are premature as they are based on untested and new standards in a rapidly changing environment, and in a context where federal debate is ongoing. We would urge the Commission to revisit these requirements, and maintain the prudent, flexible approach that has worked well for over fifteen years.

Thank you for the opportunity to comment, and for your consideration of these views. We would welcome the opportunity to further discuss these issues with the Commission.

Sincerely,

/s/

Bradley Miller

Director, Regulatory Affairs

National Automobile Dealers Association

APPENDIX A

NADA COST STUDY: AVERAGE COST PER U.S. FRANCHISED DEALERSHIP		
Proposed Change[i]	**One-Time Up-Front Cost**	**Annual Cost**
Proposed Paragraph (a) – Appointing a CISO to increase program accountability.	$27,500	$51,000
Proposed Paragraph (b) – Requiring that the Information Security Program Be Based on a Written Risk Assessment.	$26,500	$26,500
Proposed Paragraph (c) (2) – Required Data and Systems Inventory	$16,750	$10,250
Proposed Paragraph (c) (4) – Requirement to Encrypt Data at Rest and in Transit.	$9,000	$8,500
Proposed Paragraph (c) (5) – Requirement to Adopt Secure Development Practices	$9,000	$37,500
Proposed Paragraph (c) (6) – Required Multi-Factor Authentication	$33,750	$18,500
Proposed Paragraph (c) (7) – Requirement to include Audit Trails.	$30,000	$18,000
Proposed Paragraph (c) (8) – Requirement to Develop Secure Disposal Procedures	$30,000	$10,800
Proposed Paragraph (c) (9) – Required Adoption of Procedures for Change Management	$30,000	$2,000
Proposed Paragraph (c) (10) – Required Unauthorized Activity Monitoring	$20,000	$29,000
Proposed Paragraph (d) – Required Penetration Testing and Vulnerability Assessments	$20,125	$23,125
Proposed Paragraph (e) – Required Employee Training and Security Updates	$2,100	$14,875
Proposed Paragraph (f) – Required Periodic Assessment of Service Providers	$14,250	$11,250
Proposed Paragraph (h) – Required Incident Response Plan	$16,000	$6,625
Proposed Paragraph (i) – Required Written CISO report	$9,000	$9,000
Total Cost Incurred/ Dealership[ii]	**$293,975**	**$276,925**
Total Cost Incurred Across All Dealerships[iii,iv,v]	**$2,236,267,825**	**$2,106,568,475**

[i] As noted above, we received a variety of estimates from IT experts and IT outsourcing and consulting services, estimating what they would charge a financial institution like a dealer (both smaller dealers and larger dealer groups) to provide the services required under each of the new proposed requirements. We also obtained current cost figures from dealers and similarly sized financial institutions - what they are currently paying for these services – to the extent they are already doing so. Our cost study reviewed all of these numbers and estimated numbers to reach a range of potential costs, based on an analysis of what the new proposals would require a financial institution to actually do. The numbers in this chart represent an average of those numbers based on this analysis. Specifically, they represent: (a) a mean average of the range of these estimates (mean of the low and high cost estimate), and; (b) a mean average of the estimated costs for smaller, single point dealerships and larger, multi-store dealership groups (which included certain estimated economies of scale due to consolidated IT systems and back office functions.) (See Supporting Data at endnote iv below). This estimate does not include all of the potential additional costs identified in the comments above, including the new IT professional required by Proposed Paragraph (e) (estimated at $75,000-100,000 year). It only includes a conservative average estimate for those requirements for which there is a clear mandate, and for which the cost study could identify a reasonable estimate based on experience with similar entities.

[ii] Again, this analysis reflects an estimate of the *new* costs that financial institutions like dealers face from the new requirements in the Notice. However, we recognize that some of these steps are taken by some dealers already, and that not every dealership will need to spend this entire amount in new spending to comply with the new requirements in the Notice. Some may need to spend far less, but some may need to spend more.

[iii] There are 16,735 franchised automobile dealers in the U.S. It is difficult to estimate how many dealerships already undertake some or all of the new requirements under the Notice. In addition, our cost analysis reveals that there will be some economies of scale for some of the new requirements such that larger dealership chains may have a lower overall per dealership cost. Therefore, in an effort to obtain an overall cost impact for franchised dealerships in the U.S., we did not simply multiply the per dealership cost estimates by the total number of U.S. franchised dealerships (16,735.) Instead, we used the average number of dealerships per "chain," which is 2.2, and divided the total number of dealerships by that number. We then multiplied this number (7,607) by the per dealership cost estimates to reach to overall cost impact on franchised dealers in the U.S. This is an imprecise estimate, but we believe it is conservative as it divides the per dealership costs by more than 50%, which likely exceeds any current compliance estimates and any economies of scale that larger dealership groups may be able to obtain with respect to some of the new requirements.

[iv] This means that a conservative estimate of the total up-front cost for all U.S. Financial Institutions is $22,362,678,250 with an additional $21,065,684,750 per year. As noted in the body of our comments, this is based on a conservative estimate of the total number of financial institutions that would need to comply with the new requirements at 10X the number of U.S. franchised dealers. We believe that there are far more than ten times as many non-franchised dealership financial institutions in the U.S. that would be affected by these new requirements but have chosen this conservative number because we are not aware of any reliable estimates.

[v] Supporting Data Showing Range of Estimates

	Small Dealer Small Dealer Estimates are based off a single site and approximately 50 employees.		**Midsize Dealer** Midsize Dealer Estimates are based on a 5 Site Dealer with a Datacenter and 50 employees a site.	
Proposed Change	**One-Time Cost**	**Annual Cost**	**One-Time Cost**	**Annual Cost**
Proposed Paragraph (a) - Appointing a CISO to increase program accountability.	$24,000	$42,000	$31,000	$60,000
Proposed Paragraph (b) - Requiring that the Information Security Program Be Based on a Written Risk Assessment.	$20,500	$20,500	$32,500	$32,500
Proposed Paragraph (c) (2) - Required Data and systems Inventory	$13,500	$9,000	$20,000	$11,500
Proposed Paragraph (c) (4) - Requirement to Encrypt Data at Rest and in Transit.	$8,000	$8,000	$10,000	$9,000
Proposed Paragraph (c) (5) - Requirement to Adopt Secure Development Practices	$9,000	$37,500	$9,000	$37,500
Proposed Paragraph (c) (6) Multi-Factor Authentication for "any individual accessing customer information"	$17,500	$6,500	$50,000	$30,500
Proposed Paragraph (c) (7) - Requirement to include Audit Trails.	$20,000	$12,000	$40,000	$24,000
Proposed Paragraph (c) (8) - Requirement to Develop Secure Disposal Procedure	$20,000	$3,600	$40,000	$18,000
Proposed Paragraph (c) (9) - Required Adoption of Procedures for Change Management	$20,000	$2,000	$40,000	$2,000
Proposed Paragraph (c) (10) - Required Unauthorized Activity Monitoring	$15,000	$26,000	$25,000	$32,000
Proposed Paragraph (d) - Required Penetration Testing and Vulnerability Assessments	$15,500	$17,500	$24,750	$28,750
Proposed Paragraph (e) - Required Employee Security Awareness Training	$1,400	$10,950	$2,800	$18,800
Proposed Paragraph (f) - Required Periodic Assessment of Service Providers	$12,000	$9,000	$16,500	$13,500
Proposed Paragraph (h) - Required Incident Response Plan	$16,000	$5,250	$16,000	$8,000
Proposed Paragraph (i) - Required written CISO report	$8,000	$8,000	$10,000	$10,000
Total Cost Incurred	**$220,400**	**$217,800**	**$367,550**	**$336,050**

Driven

NADA MANAGEMENT SERIES L60

NADA/NAMAD/AIADA

Voluntary Protection Products: A Model Dealership Policy

NADA NATIONAL AUTOMOBILE DEALERS ASSOCIATION

This management guide has been prepared for informational purposes to assist dealerships in presenting their Voluntary Protection Products (VPPs) in a fair, ethical and legally compliant manner. Nothing in this guide, including the appendices, is intended as legal advice. Furthermore, each dealership should consult an attorney who is familiar with federal and state law applicable to VPPs and the dealership's operations before deciding whether and how to adopt this optional VPP policy. The presentation of this information is not intended to encourage concerted action among competitors or any other action on the part of dealers that would in any manner fix or stabilize the price or any element of the price of any good or service.

Driven

NADA/NAMAD/AIADA

Voluntary Protection Products: A Model Dealership Policy

TABLE OF CONTENTS

NADA/NAMAD/AIADA

Voluntary Protection Products: A Model Dealership Policy

Introduction

Among the many products and services that automobile and truck dealerships offer their customers are voluntary products designed to protect their customers' investment in the vehicles they purchase or lease.

When offered, sold, and administered in a professional and consumer-friendly manner, these voluntary protection products (VPPs) can offer customers valuable protection against an unexpected and potentially costly event such as a flood, hail damage, theft, vandalism, vehicle accident, mechanical breakdown or the customer's death, disability, or unemployment. In addition to the economic protection they provide, VPPs also can offer customers—particularly those who live paycheck to paycheck or who otherwise cannot self-insure—peace of mind knowing that the occurrence of such an unexpected event will not prevent them from keeping current on their financial obligations.[1]

Conversely, to the extent VPPs are not offered, sold, and administered in a professional manner, they can fail to provide these valuable protections, confuse and create a false sense of security for customers, result in litigation and/or administrative enforcement actions against the dealership, and undermine the goodwill of the dealership in the community.

Consequently, it is essential that dealerships strive to develop an approach toward VPPs that ensures they are offered, sold, and administered in an ethical, lawful, transparent, professional, and consumer-friendly manner. This requires that dealerships engage in several proactive steps such as conducting product research, employee training, and sales oversight, and executing their post-sale responsibilities. However, this process all begins with articulating a clear, straightforward VPP policy that provides a framework for the dealership's VPP activities. The *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy*[2] provides an optional policy template that is intended to assist a dealership with this process.

ESSENTIAL STATE LAW CONSIDERATIONS

Several states impose VPP requirements that address one or more components of this optional policy template. Some of these requirements could make portions of the policy template inapplicable to—or not prudent to adopt for—dealerships operating in those states. It is essential that dealerships review communications from their state dealer associations concerning such requirements and consult with legal counsel to determine whether—and to what extent—they should adopt the policy template.

[1] In April 2017, AAA cited a new study indicating that "64 million American drivers would not be able to pay for an unexpected vehicle repair without going into debt" and noted that "the average repair bill is between $500 and $600."

[2] For ease of reference, this title will be used to refer to *NADA/NAMAD/AIADA Voluntary Protection Products: A Model Dealership Policy.*

Instructions for Completing the VPP Policy Template

GENERAL INSTRUCTIONS AND DISCLAIMERS

Coverage and Approach

The *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* template applies to optional products that a dealership offers to its customers to protect their investment in vehicles being purchased or leased.

The policy template is structured to:

i. have the dealership provide upfront a prominent poster informing customers of the optional nature of VPPs and the dealership's commitment to providing information about each VPP before a customer decides to purchase it;

ii. state the dealership's commitment to legal compliance, training, and interdepartment coordination to effectively carry out the dealership's VPP policy; and

iii. provide a sequential list of duties the dealership will execute throughout the life cycle of VPPs, from their selection to their pricing, advertisement, presentation, sale, and, if applicable, cancellation and any customer complaints pertaining to them.

Relationship to *NADA/NAMAD/AIADA Fair Credit Compliance Policy & Program*

The *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* template is separate from—but entirely consistent with—the NADA/NAMAD/AIADA Fair Credit Compliance Policy & Program template.

The *NADA/NAMAD/AIADA Fair Credit Compliance Policy & Program* provides an optional template for developing a policy—and a detailed program to implement that policy—to promote compliance with the Equal Credit Opportunity Act (ECOA). It primarily focuses on one item (dealer participation, which is the portion of the finance charge that a dealership retains for originating a finance contract), one element of that item (pricing), and one of several statutes governing that item (ECOA), and is modeled on a consent order that the Department of Justice (DOJ) entered into with two automobile dealerships in 2007 to resolve allegations of ECOA violations.

Conversely, the *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* template focuses on multiple products (service contracts, GAP coverage, and other VPPs), multiple elements of those products (selection, pricing, advertisement, presentation, sale, cancellation, and customer complaints), multiple statutes governing those products (ECOA, the federal prohibition on unfair and deceptive acts or practices—UDAP—and other federal laws), and is not modeled on a government consent order with automobile dealerships.

These differences suggest that policy template documents for these items (dealer participation and VPPs) may need to differ. Accordingly, the *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* template is (i) broader in coverage than its fair credit counterpart (applying to the vast array of products and product elements mentioned above), and (ii) not as deep as its fair credit counterpart (as a detailed approach to compliance in a nationwide template would be difficult given the widespread differences in the state regulatory regimes and provider contractual requirements that govern these products). The *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* template therefore is more general in nature and is designed to give a dealership that chooses to adopt it a general framework for VPPs without including an extensive series of detailed requirements that may be inapplicable in a dealership's state and/or that may not fit a dealership's product offerings.

Notwithstanding the different approaches to the fair credit and VPP policy templates, they are designed so that both may be adopted by a dealership, and a dealership that chooses to adopt both may conclude that its Fair Credit Compliance Program Coordinator should also oversee the development and implementation of its VPP Policy. In addition, both templates adopt a standardized approach to pricing with a dealership that chooses to adopt the VPP policy establishing a standard retail price for its VPPs (to the extent it has discretion to do so) and only deviating from its standard retail price for pre-established, legitimate business reasons. Additionally, a dealership may conclude that it should adopt other aspects of the fair credit policy and program template that are not included in the VPP policy template, such as having the dealership's board of directors or other governing officer formally approve the policy and having the person who is responsible for executing the policy conduct periodic compliance audits and submit annual compliance reports to the board of directors or other governing officer.

Disclaimers

The *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* is an optional template that is not mandated by federal law and has not been adopted by any federal agency as a means of satisfying the requirements of federal law. In addition, as noted above, as a template that is being made available to dealerships across the country whose operations and state laws vary significantly, portions of the template may not be applicable to—or prudent to adopt by—an individual dealership. For these reasons, it is essential that each dealership consult with legal counsel who is familiar with its operations to determine whether —and to what extent—it should adopt the *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* template.

SPECIFIC INSTRUCTIONS FOR USING THE VPP POLICY TEMPLATE

Overview

This paragraph generally describes the purpose and scope of the VPP Policy.

It also contains a footnote stating that the policy does not confer any rights, benefits, or remedies to any person, except that it may be used by the dealership to discipline employees who do not comply with its terms. This is intended to forestall a third party from bringing a legal action against the dealership for a violation of the policy.

Section I. Policy Statement

This section states that the dealership will prominently display to customers a poster stating that (i) VPPs offered by the dealership are optional and are not required to purchase or lease a vehicle or obtain warranty coverage, financing, financing on particular terms, or any other product or service offered by the dealership, and (ii) the dealership is fully committed to providing customers with the price, terms, and conditions of each VPP before they decide to purchase it. The sample poster at Appendix A is available for this purpose.

The dealership should consult with its counsel concerning whether the poster should be adopted and, if so, the language it should contain. For example, if the dealership already displays a poster with similar or related language, the creation of an additional poster could be distracting or otherwise create confusion. However, it is essential that customers understand that the VPPs offered to them are completely optional.

Section II. Legal Compliance, Training, Coordination, and Document Retention

Section II.a states the dealership's commitment to complying with all applicable legal requirements,

including governing statutes, regulations, and contracts with third parties. This applies to both:

i. requirements applicable to customers, such as (a) ECOA's prohibition against discrimination on a prohibited basis, (b) the Truth in Lending Act's disclosure requirements applicable to VPPs, (c) federal and state prohibitions on unfair and deceptive acts or practices; and (d) state requirements applicable to retail installment sales and leases, VPPs that are insurance products under state law, and licensing and other requirements applicable to VPPs; and

ii. requirements applicable to other businesses, such as contractual obligations to VPP providers pertaining to remitting premiums, registering contracts, and verifying the payment of refunds.

Sections II.b and II.c state that the dealership will (i) conduct initial and periodic training of—and oversee—its employees involved in the VPP sales process, and (ii) coordinate within its departments as necessary to ensure its VPP Policy is properly carried out. An element of the oversight process could include periodically spot-checking or reviewing a sample of vehicle sales or leases entered into with customers to ensure the dealership's transactions comport with this policy. Training, oversight, and coordination are essential as the development of a policy document—by itself—will not give effect to the policy. Rather, this can only occur if the dealership takes the necessary steps to implement and maintain it.

Section II.d states that the dealership will retain records used to demonstrate compliance with this policy for an appropriate period. This should include the VPP Certification Form referenced below as well as other records documenting the completion of the various elements of this policy. The dealership should consider retaining such documents for the greater of (i) any records retention period under federal and state law for the VPPs it offers,[3] and (ii) the statute of limitations under federal and state law for violations involving those products.[4] The dealership should consult with counsel concerning the appropriate records retention period for these documents.

Section III. Product Selection

This section sets forth criteria for determining whether a particular product will be included in the dealership's VPP offerings to customers. In making this determination, the dealership should only engage reputable VPP providers, and the dealership should have confidence in the value that the product offers to customers. While a dealership may determine that additional or other criteria should be used, the following criteria in the policy template should assist the dealership with this analysis:

a. *Cost, coverage, limitations, and other terms and conditions.* The dealership should understand how a product's features offer protection of the customer's investment and whether its coverage is already provided by another product being purchased by the customer.

b. *Claims payment process.* The dealership similarly should understand the ease with which customers can file claims and receive the product benefits when a triggering event occurs. It is essential that customers have a clearly defined path to receiving such benefits. The same applies to the customer's ability to cancel and obtain any available refund for a product.

c. *Financial ability to provide product benefits.* The dealership should also consider the financial ability of the VPP provider to provide the product benefits. While this may be self-evident for many VPP providers, with others it may be prudent to inquire into their ability to pay claims.

Of course, other factors such as known reputational concerns stemming from customer complaints or litigation should not be ignored.

The analysis the dealership conducts is not intended to validate or guarantee the services provided by its VPP providers. Rather, as with vendors that dealerships retain, it is prudent to review the quality of the company, the products and services it provides, and the terms and conditions of the provider-dealer contract as part of the VPP selection process.

[3] The federal records retention requirements applicable to documents retained by automobile and truck dealerships are set forth in NADA's *A Dealer Guide to Federal Records Retention and Reporting*. Consult your state automobile dealers association concerning any applicable state records retention requirements.

[4] Among the federal laws that are most likely to apply to the sale of a VPP (e.g., ECOA, Truth in Lending Act, Federal Consumer Leasing Act, and Section 5 of the Federal Trade Commission Act), ECOA has the longest statute of limitations which generally is five years after the occurrence of a violation. See 15 U.S.C. § 1691e(f). Consult your state dealer association concerning applicable statutes of limitations under state law.

Section IV. Product Pricing

This section establishes the manner in which the dealership will determine the retail price for each VPP it offers to customers for which pricing discretion exists. For example, pricing discretion does not exist for—and this section therefore does not apply to—a VPP that is defined as an insurance product under state law and that must be offered to customers at an amount that has been established by the state insurance commissioner. Pricing discretion also may not exist as a result of—or may be limited by—other provisions of state law or policies of the VPP provider.

Where pricing discretion does exist, Section IV.a states that the dealership will establish a standard retail price (SRP) for each VPP and each bundle of VPPs it offers to customers. The dealership should sell the VPP or VPP bundle at its SRP unless one of the reasons set forth in Section IV.b for discounting that price is present in the transaction. (Section IV.c clarifies that the limitation on discounts in Section IV.b does not preclude the dealership from establishing an SRP for a bundle of VPPs that is less than the combined sum of the SRP of each individual VPP in the bundle.)

Section IV.b identifies five good-faith, competitive reasons unrelated to the customer's background that, if present, allow the dealership to sell a VPP or VPP bundle at a price that is lower than its SRP for that product or bundle. These reasons (which are set forth and described below) are among the allowable reasons for discounting a standard dealer participation rate in credit offers to customers that were (i) included in 2007 consent orders that DOJ entered into with two dealerships to resolve allegations of credit pricing discrimination, and (ii) incorporated into the *NADA/NAMAD/AIADA Fair Credit Compliance Policy & Program* as allowable reasons for discounting a standard dealer participation rate in credit offers to customers. Dealerships should be able to identify additional or different pre-established reasons for discounting the SRP it has established for a VPP or VPP bundle provided they are limited to good-faith, competitive factors that are completely unrelated to the customer's background. However, as explained in the *NADA/NAMAD/AIADA Fair Credit Compliance Policy & Program*, dealerships should proceed cautiously in allowing discounts that differ from those listed in the DOJ consent orders.

Section IV.d states that the dealership will establish procedures for recording, reviewing for corrective action, and retaining determinations that a pre-established, legitimate business reason supported a decision to discount the SRP the dealership has established for a VPP (or VPP bundle), and that the dealership will utilize the Voluntary Protection Products Certification Form at Appendix B for this purpose. (As noted below, if the dealership has another mechanism to record such discounting decisions, it would not need to adopt the VPP Certification Form at Appendix B to carry out this policy.) In order to implement these requirements, the dealership should consider adopting the following:

PRICE NEGOTIATIONS

Nothing in the model policy or these instructions is intended to foreclose price negotiations that can result in lower prices to customers for VPPs if a dealership chooses to allow them. Rather, as noted in the Introduction, the model policy and instructions are intended to promote the offering, sale, and administration of VPPs in an ethical, lawful, transparent, professional, and consumer-friendly manner. As part of this process, a dealership could allow price negotiations for VPPs while adopting and implementing appropriate procedures to ensure those negotiations are conducted in a fair and non-discriminatory manner. Alternatively, the dealership could adopt an approach that does not involve price negotiations such as the approach discussed in this section.

a. *VPP Certification Form.* The dealership should use the VPP Certification Form to record VPP discounting decisions. If the dealership does not discount any VPP or VPP bundle (i.e., if the customer pays the SRP for each VPP or VPP bundle that he or she selects), it is not necessary to execute the VPP Certification Form. The dealership should modify the VPP Certification Form template at Appendix B to reflect the dealership's specific circumstances and it may be possible, in consultation with a menu and/or software provider, to forgo the use of the VPP Certification Form by incorporating the information it contains into the menu described in Section VI.c of this policy. However, it is important to note that while the menu is presented to customers, the VPP Certification Form is intended solely as an internal dealership document to record the legitimate business reason for a VPP or VPP bundle discount.

Because the customer may choose to purchase more than one VPP and it could be unwieldy to complete a separate certification form for each VPP that the customer purchases, the VPP Certification Form at Appendix B includes a table that allows a dealership to record on a single form the pricing determination applicable to the sale of one or more VPPs to a customer.

The VPP Certification Form at Appendix B is structured in the following manner:

1. *Buyer/Lessee Information.* The top section of the form identifies the buyer(s) or lessee(s) and other transaction-specific information such as the date of the VPP sale and the VIN of the vehicle being purchased or leased. The dealership should replace or add to these data fields as necessary to reflect the information it uses to identify a vehicle delivery (such as by adding the stock number or deal number).

2. *Pricing Determination Table.* A table appears below the Buyer/Lessee Information that includes the following columns:

   A. *Name of VPP.* This column should include a preprinted listing of all VPPs or VPP bundles offered by the dealership (with the information in the columns to the right only filled in for VPPs purchased by the customer) or, alternatively, a listing of only those VPPs or VPP bundles purchased by the customer.

   B. *Standard Retail Price.* This column states the SRP for each listed VPP and VPP bundle.

For many VPPs or VPP bundles, it may be possible to preprint this price.

For others, such as an extended service contract where a dealership has established standard pricing but the SRP differs based on the deductible amount, length of coverage, or other selections made by the customer, the SRP may need to be entered after the customer has made the necessary selections. The dealership should consult with software vendors to determine how it may enter an SRP when such variables are present.

C. *Selling Price.* This is the price the customer paid for the VPP or VPP bundle. As noted above, it is only necessary to use the VPP Certification Form when the Selling Price for a VPP or VPP bundle is less than the SRP.

D. *Number of Allowable Discount.* After entering a Selling Price that is less than the SRP, the Number of the Allowable Discount from the list of Allowable Discounts that appears below the table should be entered. For example, if the Selling Price had to be discounted due to a payment cap imposed by the finance source that took assignment of the credit contract, then "1" should be entered.

E. *Discount 2.* If the SRP was discounted because the customer stated a monthly payment constraint in a fixed dollar amount that would preclude the customer from accepting a VPP or VPP bundle at the SRP, then the amount of the monthly payment constraint stated by the customer should be entered in this column. Otherwise, nothing should appear in this column.

F. *Discount 3.* If the SRP was discounted because the customer stated that he or she had access to a lower price for the same or similar VPP, then the name of the entity that offered the competing product and the price of the product stated by the customer should be entered in this column. Otherwise, nothing should appear in this column.

3. *List of Allowable Discounts.* Below the Pricing Determination Table is a list that contains the number and identification of each of the five allowable discounts (discussed in greater detail below) under the *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy.* As noted above, an adopting dealership may determine that fewer or additional pre-established discounts are allowed for good-faith, competitive reasons that are unrelated to the customer's background, but such

dealerships should consult with counsel before adding to the list of allowable discounts.

4. *Selling Employee's Certification.* Below the list of Allowable Discounts is a certification that should be signed and dated by the dealership employee who arranged the sale of the VPP(s) to the customer.

5. *Reviewer Certification.* A Reviewer's Certification is set forth in a separate box on the VPP Certification Form. Within two business days of—or another specified time period shortly after—the transaction, a senior manager who was not involved in the transaction should review the VPP Certification Form completed by the Selling Employee and any other required substantiating documentation to ensure that each VPP or VPP bundle sold to the customer was priced in accordance with this policy. (As noted above, a dealership that has also adopted the *NADA/NAMAD/AIADA Fair Credit Compliance Policy & Program* should consider designating its Program Coordinator under that program as the reviewer of its VPP Certification Forms.) If the reviewer determines that this policy was not followed, the reviewer should initiate appropriate corrective action as it relates to the customer, the employee who arranged the VPP sale, or otherwise, and record such action on the VPP Certification Form. The reviewer should then sign, date, and retain the document.

b. *Supporting Information & Document Retention.* For each allowable discount from the SRP, the dealership should clearly state the prerequisites that must be present in order to apply that discount and retain in the deal jacket or other specified location the VPP Certification Form and, if applicable, other supporting documentation. At a minimum, the documentation should include:

1. *Pricing or Payment Cap.* For the first discount, a pricing cap imposed by state law or a payment cap imposed by the company providing financing for the purchase serves as an allowable basis to discount the SRP to the pricing cap level. Documentation of—or reference to—the applicable pricing or payment cap serves as documentation for this discount.

2. *Monthly Payment Constraint.* For the second discount, a monthly payment constraint in a fixed dollar amount stated by the customer that precludes the dealership from selling a VPP or VPP bundle at its SRP serves as an allowable basis to discount the SRP to the level that allows the customer to purchase the VPP or VPP bundle. The VPP Certification Form records this information and therefore serves as appropriate documentation for this discount.

3. *More Competitive Offer.* For the third discount, a more competitive offer for the same or similar VPP to which the customer states that he or she has access serves as an allowable basis for the dealership to discount the SRP to the level necessary to either meet the competing offer or beat the competing offer by a certain set amount. (In order to promote consistent discounting decisions, the dealership should determine, as a matter of policy, whether it will offer to meet competing offers or beat competing offers by a set amount.) The VPP Certification Form records this information (the name of the VPP provider and the price of the VPP) and therefore serves as appropriate documentation for this discount. **As part of this process, the dealership should not seek to verify the existence of a more competitive offer by contacting the competitor.**

4. *Promotional Pricing.* For the fourth discount, a promotional program that allows all customers to receive a VPP or VPP bundle at a discounted price serves as an allowable basis to discount the SRP pursuant to the terms of the promotional program. The dealership advertisement or other communication identifying the terms of the promotional program serves as appropriate documentation for this discount.

5. *Employee Pricing.* For the fifth discount, a dealership employee incentive program that allows employees to receive a VPP or VPP bundle at a discounted price serves as an allowable basis to discount the VPP or VPP bundle pursuant to the terms of the program. The dealership employee incentive program or reference to it serves as appropriate documentation for this discount.

Section V. Product Advertisement

This section states that the dealership will not advertise, solicit, or otherwise market VPPs in a manner that is deceptive, misleading, confusing, or otherwise inconsistent with their terms and conditions. While all areas addressed by the *NADA/NAMAD/AIADA Model Dealership Voluntary Protection Products Policy* can invite scrutiny by regulators, this area in particular has witnessed several recent enforcement actions by federal agencies alleging that finance sources, VPP providers, and dealers have deceptively marketed VPPs to consumers.[5] It is essential that the dealership have a process in place to review all forms of marketing (e.g., newspaper and internet ads, YouTube videos, emails, text messages, social media, signage at the dealership, etc.) to ensure its marketing materials comport with this section.

Section VI. Product Presentation and Sale

This section establishes a process for ensuring that customers are fully informed about the features, optional nature, and price of VPPs before deciding to purchase them.

a. Section VI.a states that the dealership will (i) ensure its employees who offer VPPs to customers fully understand their benefits, limitations, and other terms and conditions before offering them to customers; and (ii) not offer products to customers for which they are ineligible or would derive no value. As with the other elements of this section, information about dealer product offerings should be a component of the VPP training that such employees receive, and customers should not be offered products

[5] Recent examples include (i) a consent order the Consumer Financial Protection Bureau (Bureau) entered into with a bank engaged in indirect vehicle financing to resolve allegations that the bank overstated to consumers the extent of coverage provided by its optional Guaranteed Asset Protection (GAP) product (*Santander Consumer USA, Inc.*, BCFP File No. 2018-BCFP-0008 (Nov. 20, 2018)); (ii) consent orders the Bureau entered into with a bank engaged in indirect vehicle financing and its non-bank partner company to resolve allegations that the respondents understated to service members the costs of optional vehicle service contracts and GAP coverage (*U.S. Bank Nat'l Ass'n*, BCFP File No. 2013-CFPB-0003 (Jun. 26, 2013) and *Dealers' Fin. Serv., LLC*, BCFP File No. 2013-CFPB-0004 (Jun. 25, 2013)); and (iii) consent orders that the Federal Trade Commission entered into with the provider of an optional bi-weekly payment product and an automobile dealership group that sold the product to resolve allegations that the respondents failed to disclose to consumers the total amount of the fees associated with the product and that those fees could offset any savings to consumers who purchased the product (*Nat'l Payment Network, Inc.*, FTC Docket No. C-4521 (May 4, 2015) and *Matt Blatt, Inc.*, FTC Docket No. C-4532 (Jul. 2, 2015)).

that would not provide value based on the circumstances of the customer's transaction (such as being offered an extended service contract on a leased vehicle whose protection is covered by the manufacturer's warranty during the lease term). During this training, employees should be reminded that while knowledge of the product and the elements of the customer's transaction are essential, dealer employees are not—and should not present themselves as—agents of the customer who are working on the customer's behalf.

b. Section VI.b states that the dealership will inform customers orally that the VPPs it offers are optional, and that the dealership will not contradict this disclosure in any way such as by stating or implying that the purchase of a VPP is required as a condition of purchasing or leasing the vehicle, obtaining warranty coverage, qualifying for financing or obtaining particular financing terms, or executing any other part of the transaction. Because this involves an oral disclosure that cannot be monitored solely through a document review, the dealership should have a process in place to monitor periodically product presentations by its employees to ensure they adhere to this requirement, and the dealership should take immediate corrective action if it learns that an employee has deviated from it.

c. Section VI.c states that the dealership will present VPPs to customers in a standard, simple menu format that, at a minimum, prominently discloses:

   1. that the purchase of any listed product is optional;
   2. that any listed product may be purchased separately;
   3. that the purchase of any listed product is not required to purchase or lease a vehicle, obtain warranty coverage, qualify for financing, or receive financing on particular terms;
   4. that the listed products or the protections they provide may be available from other sources;
   5. that the dealer may retain a portion of the sale price of the listed products;
   6. the price of—and monthly payment for—the vehicle without the purchase of a VPP;
   7. the price of—and monthly payment for—each product if purchased separately; and
   8. the price of—and monthly payment for—each product bundle if products are purchased as a bundle.

   By making these disclosures prominently, dealers provide useful information that facilitates the customer's understanding of the price, optional nature, and potential availability from other sources of—and the dealer's economic interest in—the VPPs being offered.

d. Section VI.d states that the dealership will present VPPs in a manner that is designed to assist customers in making informed purchasing decisions by presenting information on the VPP's price, deductible, limitations, benefits, eligibility, requirements for maintaining coverage, claims process, cancellation and refund rights and procedures, and other important terms and conditions. Section VI.e further states that prior to the sale of a VPP, the dealership will provide the customer with a copy of—and an opportunity to review—each purchased VPP's terms and conditions as well as other required disclosures and request the customer's acknowledgement that he or she has received the menu disclosures and elected to (i) purchase each selected VPP or VPP bundle, or (ii) decline purchasing any VPP or VPP bundle.

   While it typically is not practical to present orally to customers all of the information about a VPP that is contained in the VPP policy document(s), dealership employees should explain to customers (i) basic product information that may inform their purchasing decision, and (ii) that the full terms and conditions applicable to the VPP are contained in the written VPP policy document(s), which the dealership employee should provide the customer—and ensure the customer has an opportunity to review—prior to the sale of the VPP. The customer should then acknowledge in writing that he or she has received the menu disclosures and elected to purchase the VPP.

e. Section VI.f states that the dealership will provide to customers all required post-sale forms. The dealership should consult with counsel to ensure that any requirement to provide such forms under state law or pursuant to the dealer's agreements with the finance or lease source and VPP provider is fulfilled.

Section VII. Product Cancellation

This section generally establishes that the dealership will facilitate both customer requests to cancel VPPs customers have purchased from the dealership and the customer's receipt of any refunds due.

Section VII.a states that the dealership will ensure customers have a simple and clear method to exercise any cancellation rights applicable to VPPs they have purchased. While state law and/or VPP provider policy documents typically specify how VPP cancellations and refunds will be administered, the dealership, as noted above, should consider the ease with which customers can exercise these rights when deciding whether to offer particular VPPs. This process should not be convoluted or unnecessarily burdensome to the customer.

Section VII.b states that the dealership will take no action to delay, prevent, or otherwise frustrate customers' exercise of such rights. This is another area that should be particularly emphasized during the employee training to carry out this policy.

Section VII.c states that the dealership will promptly and courteously process customer cancellation requests and issue, or facilitate the issuance of, refunds due to customers or to the finance or lease source, as required. If the dealership is responsible for providing such refunds, then the dealership should have a process in place to process the refund request without delay. If the dealership is not responsible for providing such refunds but the dealership nonetheless receives a cancellation request from a customer, the dealership should provide information to the customer on how to exercise his or her cancellation right.

Section VII.d states that the dealership will maintain, or send to the VPP provider, verification that the refund was provided to the customer or to the finance or lease source, as required, if the dealership issues the refund. Because multiple parties may be involved in the sale, financing, and administration of VPPs to customers, it is incumbent on all parties (the dealership, the finance or lease source, and the VPP provider) to communicate with one another to ensure customer cancellation requests have been honored. The dealership should

review state law as well as its contract with the finance or lease source and VPP provider to ensure it is fulfilling any obligations in this regard.

Section VIII. Customer Complaints

This section states that the dealership will promptly and courteously respond to customer complaints regarding VPPs purchased from the dealership. While robust training, transparency, clear communications, responsiveness, and oversight should greatly diminish the likelihood of customer complaints regarding VPPs, the dealership should nonetheless be prepared to handle customer complaints that may arise (both as a complaint applies to the individual transaction involved and any systemic problems that the complaint may reveal). Developing the following procedures is one way to assist the dealership in addressing customer complaints:

a. Assign an appropriate dealership manager with responsibility for overseeing the dealership's customer complaints process;

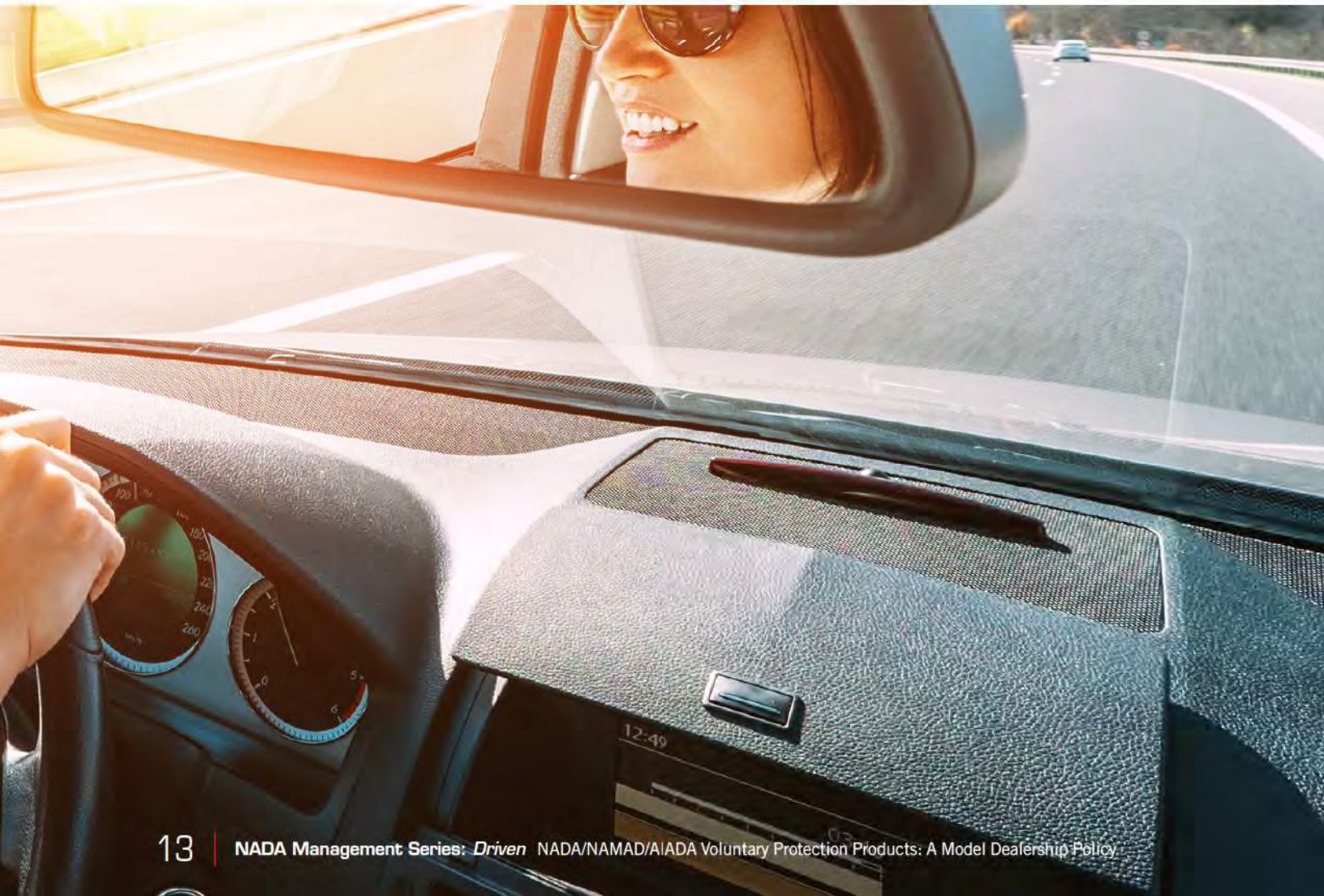
b. Ensure customers are provided with the name and phone number of the dealership manager to contact if they have a complaint;

c. Establish a process for logging in customer complaints;

d. Direct the manager with oversight responsibility to handle the customer complaint or refer it to another dealership employee to (i) determine how the complaint can be resolved, and (ii) attempt to resolve the complaint; and

e. Record (i) the resolution of the complaint and whether the customer is satisfied with the resolution, or (ii) the reason it cannot be resolved.

As with other aspects of this policy, the development of a customer complaint process should be tailored to the dealership's circumstances. However, if the dealership develops an effective customer complaint process (which should be in place for all of the dealership's departments), it will help the dealership address customer concerns in their early stages, enhance its business processes, and further demonstrate its commitment to a fair, ethical, and legally compliant VPP sales process.



Templates

[*Name of Dealership*] Voluntary Protection Products Policy

OVERVIEW

Among the many products and services that the Dealership offers its customers are voluntary products that are designed to protect the customers' investment in the vehicles they purchase or lease. These voluntary protection products (VPPs) can provide great value to customers when they are offered in a fair and transparent manner and customers fully understand their costs, benefits, and limitations. In order to facilitate a compliant, professional, and consumer-friendly VPP sales process, the Dealership adopts the following Policy:[1]

I. POLICY STATEMENT

The Dealership will prominently display the poster at Appendix A, within clear view of prospective customers, stating that (i) VPPs offered by the Dealership are completely optional and are not required to purchase or lease a vehicle or to obtain warranty coverage, financing, financing on particular terms, or any other product or service offered by the Dealership, and (ii) the Dealership is fully committed to providing customers with the price, terms, and conditions of each VPP before they decide to purchase it.

II. LEGAL COMPLIANCE, TRAINING, OVERSIGHT, COORDINATION, AND RECORDS RETENTION

a. The Dealership will fully comply with federal, state, and local law (including applicable licensing and insurance requirements and the prohibition against discrimination on a prohibited basis) as well as contractual obligations the Dealership has entered into with VPP providers, finance and lease sources, and other third parties.

b. The Dealership will conduct initial and periodic training on this Policy for—and oversee—Dealership employees involved in VPP selection, pricing, advertisement, presentation, sales, cancellation, and customer complaints.

c. The Dealership will coordinate the efforts of its departments to ensure a consistent and harmonized approach toward the proper execution of this Policy.

d. The Dealership will retain records used to document compliance with this Policy for an appropriate period.

III. PRODUCT SELECTION

The Dealership will only offer to customers VPPs that offer value. At a minimum, to the extent it is available, the Dealership will consider:

a. the product's cost, coverage, limitations, and other terms and conditions;

b. the product's claims payment and cancellation process; and

c. the product provider's financial ability to provide the product benefits.

IV. PRODUCT PRICING

a. The Dealership will establish a Standard Retail Price (SRP) for each VPP and each bundle of VPPs it offers for which pricing discretion exists.

b. The Dealership will only discount the SRP for the following pre-established, legitimate business reasons:

1. a pricing or payment cap imposed by law or by the company providing financing for the purchase;
2. a customer's stated monthly payment constraint;
3. a more competitive offer for the same or similar VPP;
4. promotional pricing for which the customer qualifies; and
5. employee pricing for which the customer qualifies.

c. The limitation on discounts in Section IV.b of this Policy does not preclude the Dealership from establishing an SRP for a bundle of VPPs that is less than the combined sum of the SRP of each individual VPP in the bundle.

d. The Dealership will establish procedures, including the utilization of the VPP

[1] Nothing in this policy, express or implied, is intended to or shall confer upon any person any right, benefit, or other remedy of any nature whatsoever under or by reason of these standards or any federal, state, or local law. However, any violation of this Policy by a Dealership employee can be the basis for disciplinary action, including termination of employment and/or the agency or independent contractor relationship.

Certification Form at Appendix B, to record, review for corrective action, and retain determinations that a pre-established, legitimate business reason supported a decision to discount the SRP.

V. PRODUCT ADVERTISEMENT

The Dealership will not advertise, solicit, or otherwise market VPPs in a manner that is deceptive, misleading, confusing, or otherwise inconsistent with their terms and conditions.

VI. PRODUCT PRESENTATION AND SALE

a. The Dealership will ensure its employees who offer VPPs to customers fully understand their benefits, limitations, and other terms and conditions before offering them to customers. The Dealership will not offer products to customers for which they are ineligible or would derive no value.

b. The Dealership will inform customers orally that the VPPs it offers are *optional*. The Dealership will not contradict this disclosure in any way, including by stating or implying that the purchase of a VPP is required as a condition of purchasing or leasing a vehicle, obtaining warranty coverage, qualifying for financing or obtaining particular financing terms, or executing any other part of the transaction.

c. The Dealership will present VPPs to customers in a standard, simple menu format that, at a minimum, prominently discloses:

   1. that the purchase of any listed VPP is optional;
   2. that any listed VPP may be purchased separately;
   3. that the purchase of any listed VPP is not required to purchase or lease a vehicle or to obtain warranty coverage, qualify for financing, or receive financing on particular terms;
   4. that the listed VPPs or the protections they provide may be available from other sources;
   5. that the dealer may retain a portion of the sale price of the listed VPPs;
   6. the price of—and monthly payment for—the vehicle without the purchase of a VPP;
   7. the price of—and monthly payment for—each VPP if purchased separately; and
   8. the price of—and monthly payment for—each product bundle if VPPs are purchased as a bundle.

d. The Dealership will present VPPs in a manner that is designed to assist customers in making informed purchasing decisions. This includes presenting to the customer information about the VPPs' price, deductibles, limitations, benefits, eligibility, requirements for maintaining coverage, claims process, cancellation and refund rights and procedures, and other important terms and conditions.

e. Prior to the sale of a VPP, the Dealership will:

   1. provide the customer with a copy of—and an opportunity to review—each selected VPP's terms and conditions as well as any other required disclosures; and
   2. request the customer's acknowledgement of the menu disclosures and election to:
      A. purchase each selected VPP or VPP bundle, or
      B. decline purchasing any VPP or VPP bundle.

f. Following the sale of a VPP, the Dealership will provide to customers all required post-sale forms.

VII. PRODUCT CANCELLATION

The Dealership will:

a. ensure customers have a simple and clear method to exercise any cancellation rights applicable to VPPs they have purchased;

b. take no action to delay, prevent, or otherwise frustrate customers' exercise of such rights;

c. promptly and courteously process customer cancellation requests and issue, or facilitate the issuance of, refunds due to customers or to the finance or lease source, as required; and

d. maintain, or send to the VPP provider, verification that the refund was provided to the customer or to the finance or lease source, as required, if the Dealership issues the refund.

VIII. CUSTOMER COMPLAINTS

The Dealership will promptly and courteously respond to customer complaints regarding VPPs purchased from the Dealership.

[*Name of Dealership*]
Voluntary Protection Products Policy

[*Name of Dealership*] offers vehicle service contracts and other voluntary products that are designed to protect your investment in a vehicle you purchase or lease from us. The purchase of any of these voluntary protection products is completely **optional** and is **not** required to purchase or lease a vehicle or obtain warranty coverage, financing, financing on particular terms or any other product or service offered by the dealership. [*Name of Dealership*] is fully committed to providing you the price, terms and conditions of each voluntary protection product before you decide to purchase it.

Appendix B

Voluntary Protection Products Certification Form

Buyer(s)/Lessee(s) Name(s) _____ Date _____ VIN _____

Name of VPP (or VPP Bundle)	Standard Retail Price	Selling Price	If Selling Price is less than Retail Price, enter the Number of the Allowable Discount from the list below.	If Discount 2 is selected, enter the Amount of the Monthly Payment Constraint.	If Discount 3 is selected, enter the Name of the Competing Offeror *and* the Price of the Competing Offer.

Allowable Discounts

Discount 1 VPP limited by pricing or payment cap

Discount 2 Customer stated monthly payment constraint

Discount 3 Customer stated competing offer

Discount 4 Customer qualified for Dealership Promotional VPP Campaign

Discount 5 Customer qualified for Dealership Employee Incentive Program

I certify that the information above is true and correct to the best of my knowledge and that any discount from the Standard Retail Price was made in good faith and in a manner that is consistent with the requirements of the [*Name of Dealership*] Voluntary Protection Products Policy.

_____
Signature

_____
Date

_____
Printed Name

_____
Title

Reviewer Certification

I have reviewed the above information and supporting documentation and:

❑ certify that the Selling Price complies with the [*Name of Dealership*] Voluntary Protection Products Policy, or

❑ certify that I have initiated the corrective action noted below.

- Reduced the customer's Selling Price for _____ to $_____ or provided a refund to the customer in the amount of $_____.
- Taken the following employee corrective action (describe):_____
  _____
- Other (describe): _____
  _____

_____
Signature

_____
Date

_____
Printed Name

_____
Title

NAMAD
NATIONAL ASSOCIATION OF MINORITY AUTOMOBILE DEALERS

NADA

AIADA®
American International Automobile Dealers Association

nada.org