GNYADA

Greater New York Automobile Dealers Association

Sponsored by Spectrum REACH AUTOMOTIVE

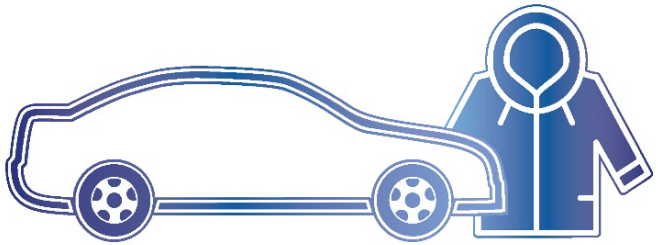
Bagels with Bieber

Spectrum REACH

AUTOMOTIVE

Contact Tim Minter 267-566-2139

GNYADA
Greater New York Automobile Dealers Association



TURN CARS INTO COATS

BRING WARMTH TO A NEW YORKER IN NEED

With the chilly air setting in and winter weather on the way, we are asking you to help New Yorkers stay warm this season by participating in GNYADA's annual coat drive.

DMV-DIRECT

REGISTRATION, TITLING, & BEYOND...

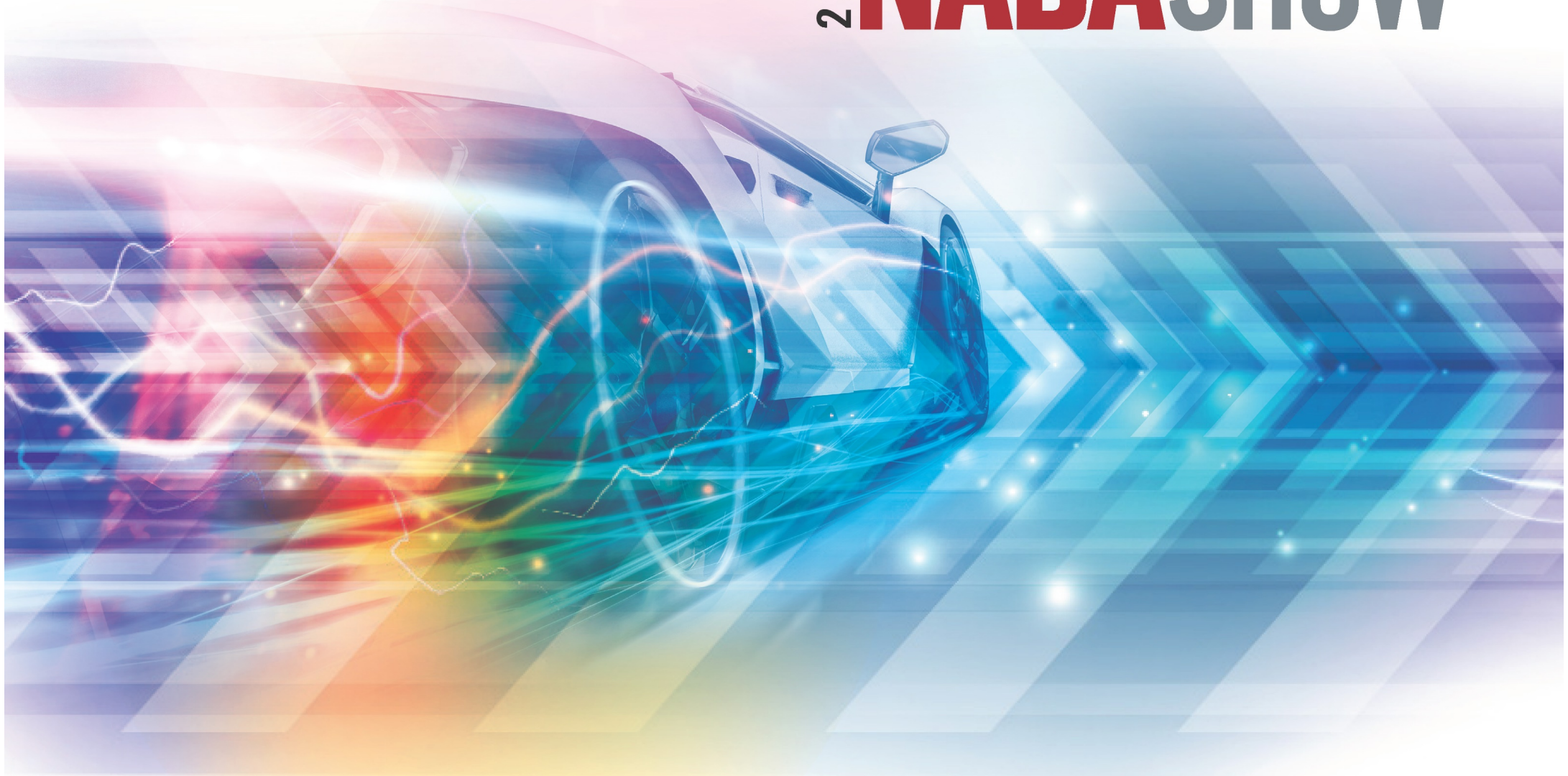
CALL 718.747.0400

GNYADA's vehicle registration and titling service, DMV-DIRECT, has been dealers go-to source for fast, convenient, & reliable DMV services.

DMV-DIRECT provides many DMV related services, including:

- Permanent Registration Issuance
- Duplicate Titles In 3 To 5 Days
- Out-of-State Registration & Title Processing for 42 States
- On-Site Connecticut Plates Issuance
- Dial-In Information Verification
- In-Transit Processing
- Duplicate Registrations
- Registration Renewals
- Title-Only Transactions
- Plate Surrenders
- Dealer Plate Renewals
- Rental Plate Renewals
- Repossessed Vehicles Processing
- MV-82 & Transmittal Forms Supplied
- Boat Registrations – Renewed and Duplicates
- Trailer Plates
- Commercial Plates

2022 NADA SHOW



EXPERIENCE THE FUTURE

NADA SHOW 2022 | LAS VEGAS | MARCH 10-13

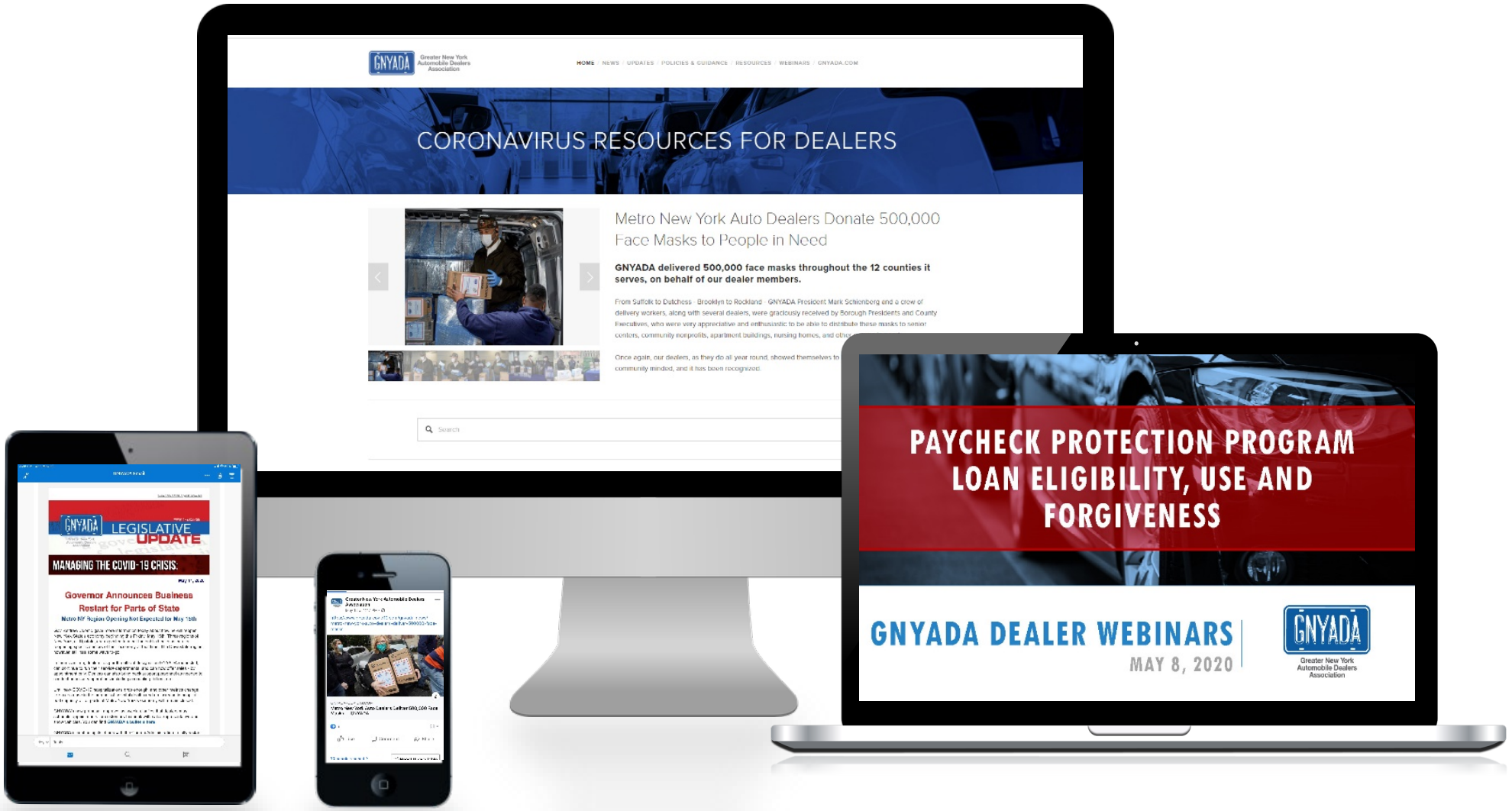
GNYADA

Greater New York Automobile Dealers Association

HUB

For more information contact:
Michael W. Conway,
GNYADA Insurance
Phone: 718-767-8100
mconway@gnyada.com

WWW.GNYADA-COVID19.COM



NATIONAL AUTOMOBILE DEALERS ASSOCIATION

Amended FTC Safeguards Rule:
Overview and Update

Brad Miller
Director Legal and Regulatory Affairs and *Senior Counsel*, Digital Affairs | NADA |
bmiller@nada.org

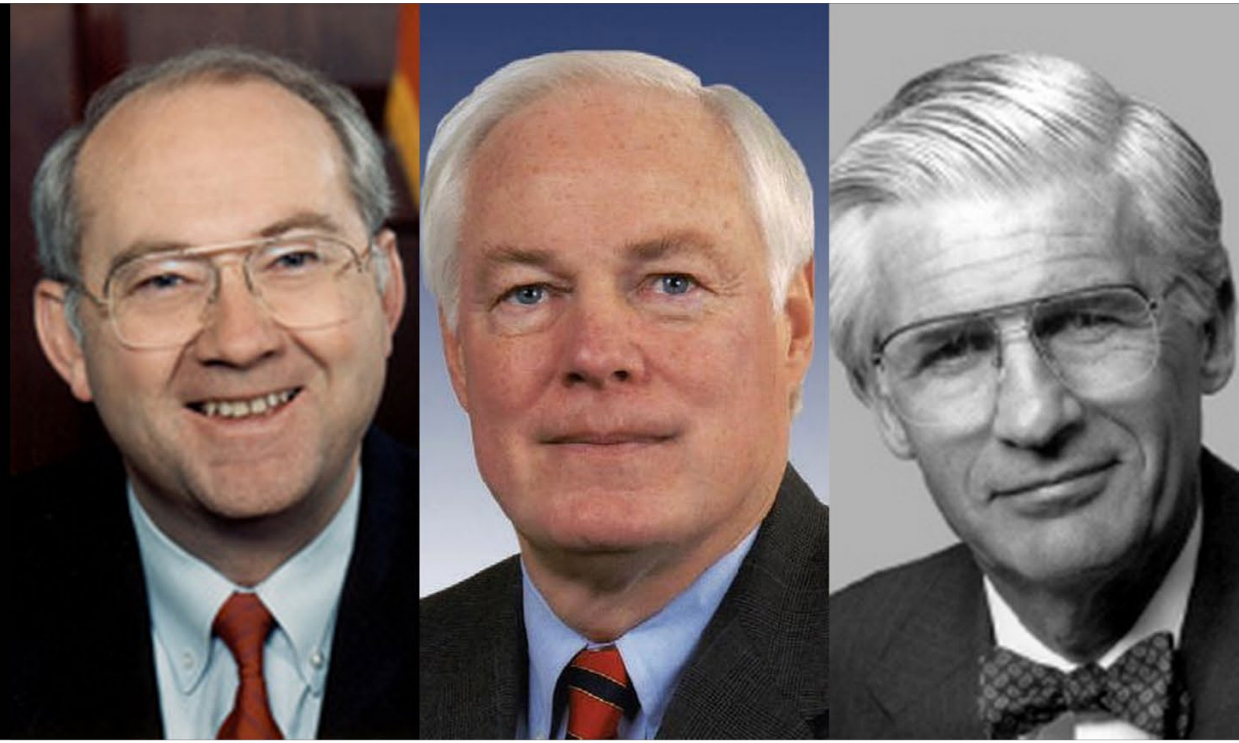
NADA

Federal Privacy and Security: Overview

The Legal Basics: Federal Law

GRAMM-LEACH-BLILEY ACT ("GLB")

- Dealers are "Financial Institutions"
- GLB Safeguards Rule – requirements to protect
- FTC Privacy Rule - restrictions on sharing with third parties



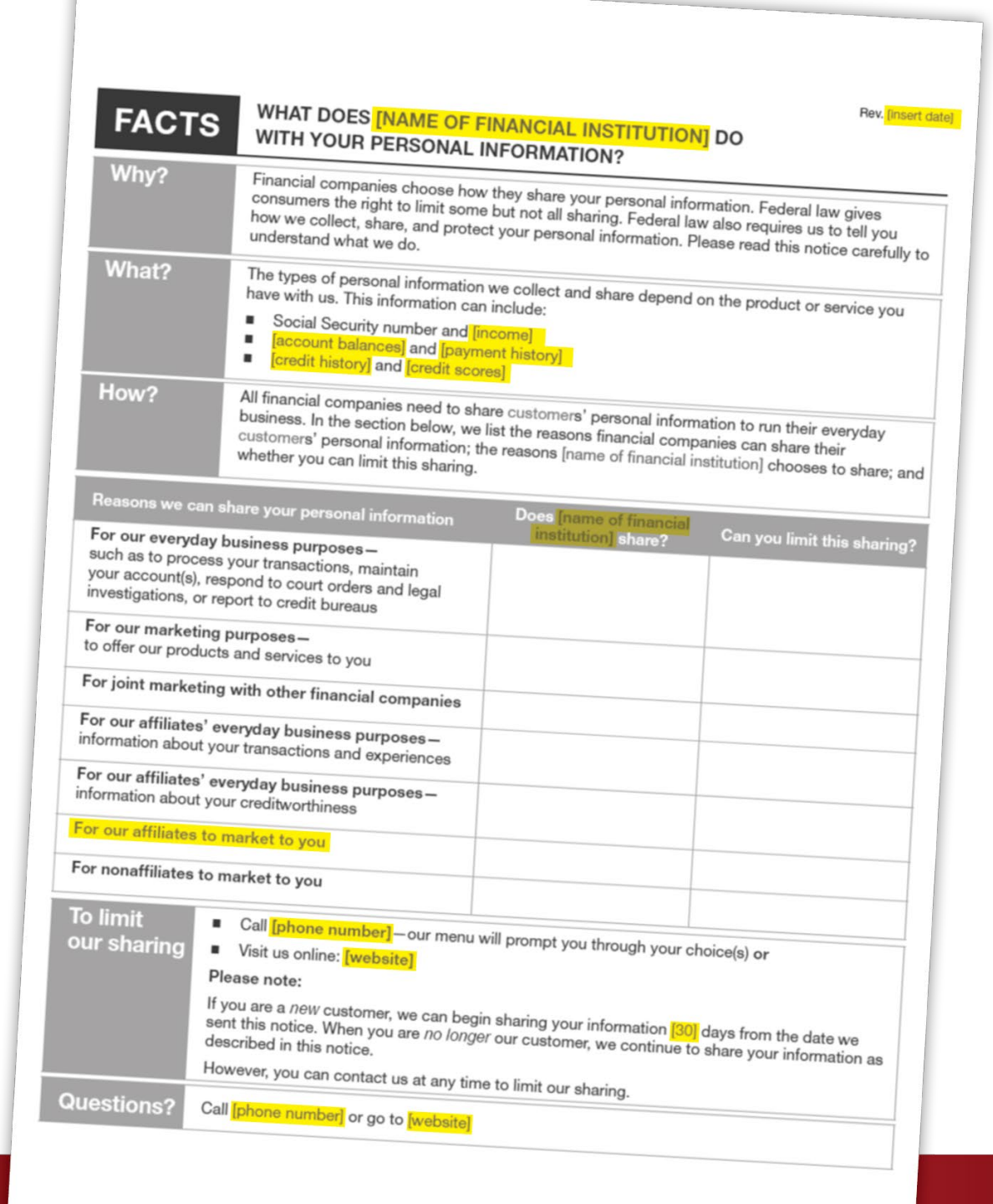
SECTION 5 FTC ACT – FEDERAL "UDAP"

- Very broad view of protected personal information

Federal Privacy Notice

MOST DEALERS

- State no sharing outside of an exception
- Practically impossible to do otherwise



FACTS WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?

Rev. [insert date]

Why? Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

What? The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and [income]
- [account balances] and [payment history]
- [credit history] and [credit scores]

How? All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing

- Call [phone number]—our menu will prompt you through your choice(s) or
- Visit us online: [website]

Please note:

If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice.

However, you can contact us at any time to limit our sharing.

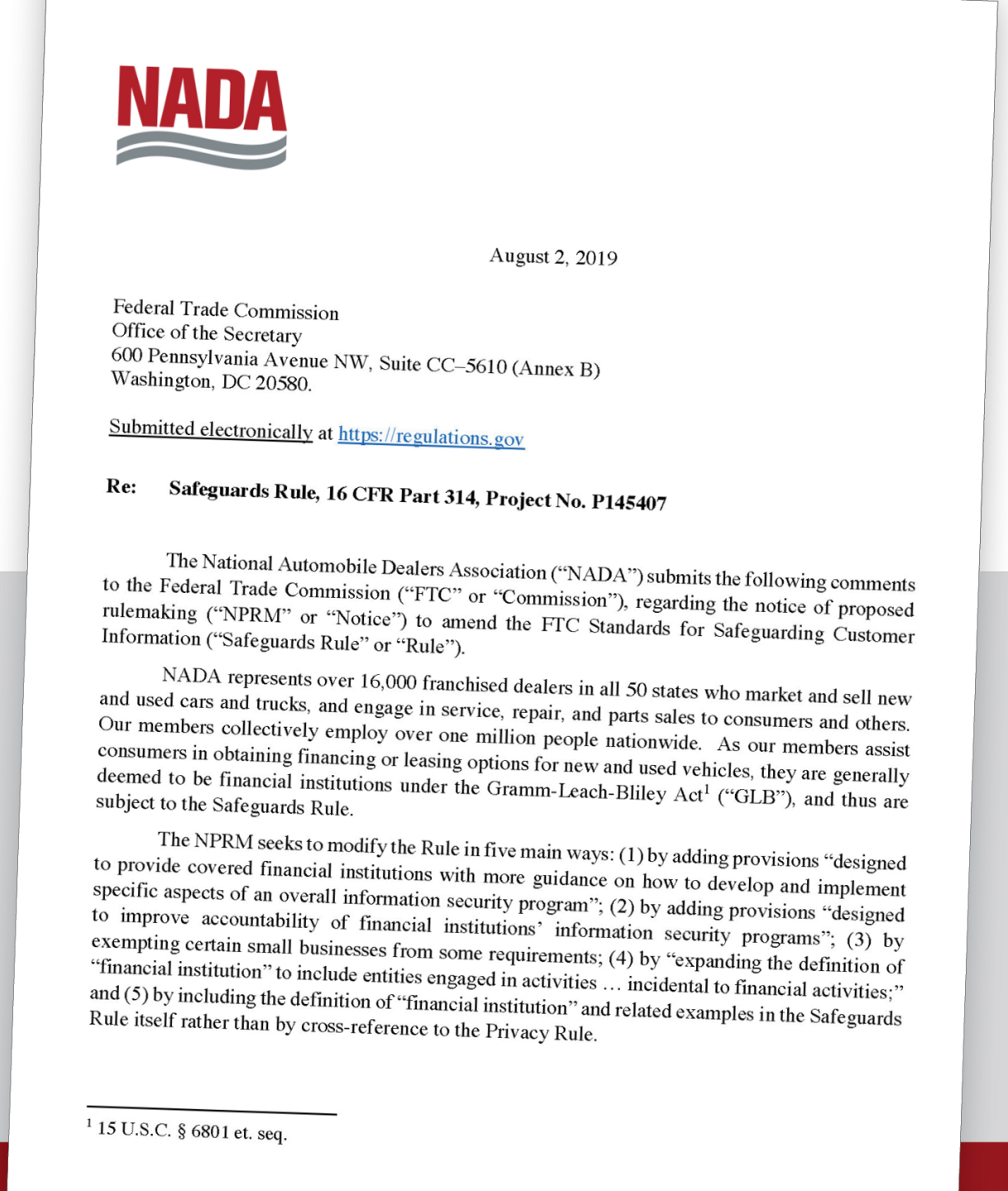
Questions? Call [phone number] or go to [website]

Proposed Amendments to the FTC Safeguards Rule

LEARN MORE

Proposed Amendments

NADA Comments



NADA

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.

Why the changes?

- In response to “a series of recent high-profile breaches”
- Increased Hill pressure
- Most prevalent consumer complaint
- New slate of Commissioners
  - Controversial 3-2 split

The FTC Transition

Lina Khan
Chairwoman (D)

Rebecca Slaughter
Commissioner (D)

Alvaro Bedoya
Expected Commissioner Nominee (D)

Noah Phillips
Commissioner (R)

Christine Wilson
Commissioner (R)

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**

Amended Safeguards Rule

Home » News & Events » Press Releases » FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches

FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches

October 27, 2021

Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses

SHARE THIS PAGE

FOR RELEASE

TAGS: Finance | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security | Gramm-Leach-Bliley Act

The Federal Trade Commission today announced a newly updated rule that strengthens the data security safeguards that financial institutions are required to put in place to protect their customers' financial information. In recent years, widespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, and other forms of financial distress. The FTC's updated Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain a comprehensive security system to keep their customers' information safe.

"Financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The updates adopted by the Commission to the Safeguards Rule detail common-sense steps that these institutions must implement to protect consumer data from cyberattacks and other threats."

The changes adopted by the Commission to the Safeguards Rule include more specific criteria for what safeguards financial institutions must implement as part of their information security program such as limiting who can access consumer data and using encryption to secure the data. Under the updated Safeguards Rule, institutions must also explain their information sharing practices, specifically the administrative, technical, and physical safeguards the financial institutions use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customers' secure information. In addition, financial institutions will be required to designate a single qualified individual to oversee their information security program and report periodically to an organization's board of directors, or a senior officer in charge of information security.

The Safeguards Rule was mandated by Congress under the 1999 Gramm-Leach-Bliley Act. Today's updates are the result of years of public input. In 2019, the FTC sought comment on proposed changes to the Safeguards Rule and, in 2020 held a public workshop on the Safeguards Rule.

In addition to the updates, the FTC is seeking comment on whether to make an additional change to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the Commission. The FTC is issuing a supplemental notice of proposed rulemaking, which will be published in the Federal Register shortly. The public will have 60 days after the notice is published in the Federal Register to submit a comment.

Today, the FTC also announced it adopted largely technical changes to its authority under a separate Gramm-Leach Bliley Act rule, which requires financial institutions to inform customers about their information-sharing practices and allow customers to opt out of having their information shared with certain third parties. These changes align the rule with changes made under the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank). Under Dodd-Frank, Congress narrowed the FTC's jurisdiction under that rule to only apply to motor vehicle dealers.

The Commission voted 5-0 to publish the final revisions to update the FTC's jurisdiction under Dodd-Frank and the supplemental notice of proposed rulemaking to the Safeguards Rule in the Federal Register. The Commission voted 3-2 to publish the revisions to the Safeguards Rule in the Federal Register. Commissioners Noah Joshua Phillips and Christine S. Wilson voted no and issued a joint dissenting statement. Chair Lina M. Khan and

EVENTS CALENDAR

Related Actions

Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter Regarding Regulatory Review of the Safeguards Rule

Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson in the Matter of the Final Rule amending the Gramm-Leach-Bliley Act's Safeguards Rule

16 CFR Part 314: Standards for Safeguarding Customer Information (Supplemental Notice of Proposed Rulemaking)

16 CFR Part 314: Standards for Safeguarding Customer Information (Final Rule)

16 CFR Part 313: Privacy of Consumer Financial Information Rule under the Gramm-Leach-Bliley Act

Media Resources

Privacy and Security Enforcement

Data Security

Amended Safeguards Rule – the "Basics"

- Abandon "reasonable" standard for list of requirements
- Must comply by December 9, 2022
- Certain requirements do not apply if < 5,000 customer records
- Increased obligations internal systems and re Third Parties

What Do the Amendments Do?

- Require:
  - Implementation of certain technical changes/tools
  - Required policy changes/updates
  - Written reports and documentation
  - Training requirements
- Does not change liability per se, still no private right of action, but:
  - Enforcement penalties – ($43,792/violation)
  - UDAP violation as basis for state claims
- Clarify that “customer record” is viewed very broadly
  - Not just SSN or CC#
  - Not even just NPPI
- Increased obligations re Third Parties

New Requirements

Qualified Employee	Written Risk Assessment	Access Controls	Data and Systems Inventory
Data Encryption	Secure Development Practices	Multi-Factor Authentication	Systems Monitoring and Logging
Secure Data Disposal Procedures	Change Management Procedures	Unauthorized Activity Monitoring	Intrusion Detection/ Vulnerability Testing
Overseeing/Monitoring Service Providers	Written Incident Response Plan	Annual Reporting to Board	

Preliminary Guidance

NADA

Amended Final Safeguards Rule
Preliminary FAQs

On October 27, 2021, the FTC issued its long-awaited, final amendments to the FTC Safeguards Rule ("Rule"). The Rule contains a significant number of new and expanded procedural, technical, and personnel requirements that financial institutions, including dealers, must satisfy to meet their information security obligations.[1]

Regulatory Affairs will develop comprehensive compliance guidance for NADA members.

In the meantime, dealers are encouraged to reach out to their technology vendors as soon as feasible to ensure they are taking the necessary steps to comply with the new requirements.

Attached are answers to several preliminary dealer questions, some details about what the Amended Rule requires (Exhibit A), and a copy of a third-party cost study commissioned by NADA that outlines the estimated costs for compliance with many of the new requirements (Exhibit B).

Q What is the Safeguards Rule?

A The Safeguards Rule ("Rule") is a federal data security rule that requires financial institutions (including dealers) to have measures in place to keep customer information secure. In addition to developing their own safeguards, dealers are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.

Q What does it require?

A The specific requirements of the current Rule are outlined in several NADA guides, but, in brief, the Rule requires financial institutions to "develop, implement, and maintain a [written] comprehensive information security program" that "contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."

In other words, you should today have a written document that you have developed for your store, after reviewing your systems and the information you maintain, that contains a series of steps you are taking to protect that data.

Notably, this current requirement allows dealers the flexibility they need to protect data in a manner that is appropriate to the size and scope of their operations.

Q Is the Safeguards Rule new?

A The Rule itself is not new; it has been in effect for nearly 20 years. What is new is that the FTC has amended the Rule. The FTC began its efforts to amend the Rule in 2019, and NADA submitted several sets of detailed comments, participated in a Public FTC workshop, and undertook extensive additional advocacy in response to the proposed amendments.

Q Why is the FTC changing the Rule?

A The FTC proposed amendments to the current Rule in response to pressure to address "recent high profile data breaches." While the FTC responded favorably to several concerns with the proposed Rule that NADA identified (including by eliminating the proposed requirement that financial institutions hire or retain a Chief Information Security officer (CISO)), it nonetheless included in the Amended Rule a series of new technical requirements.

1 The Amended Rule is final, but in connection with the proposed rule, the FTC is also considering a proposal that financial institutions notify the Commission of detected "security events." (Defined as "an event resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system.") The Commission is issuing a Notice of Supplemental Rulemaking that proposes adding such a requirement. NADA will be submitting comments to the FTC and will provide further guidance as it becomes available.

Q What has changed?

A Some of the specific changes are listed in Appendix A below but, broadly speaking, the Amended Rule modifies the current flexible approach to data security by mandating a list of requirements that all financial institutions (including dealers) must meet, regardless of their size, systems, or the types or scope of data they maintain.

This means that for a dealer to comply with the Amended Rule, the dealer must take each of the steps and actions outlined in the Amended Rule—without any determination as to the security benefit of those actions.

In addition, dealers must ensure that any of their vendors that access any customer data must also comply with these same requirements, and dealers must audit them for compliance. If a dealer is unable to do so, the FTC has said that the dealer may no longer engage that vendor.

Q When is this effective?

A Dealers, and all of their service providers that access any customer data, will have one year from the Amended Rule's publication in the Federal Register (which is expected shortly) to comply with the majority of the new requirements.

Some of the changes in the Amended Rule take effect 30 days after publication. Although the Commission notes that "These remaining requirements largely mirror[] the requirements of the existing Rule." However, as dealer action may be necessary on several of these changes in the next 30 days, dealers should consult with their counsel to ensure compliance with the current rule and any such changes.

The sections that require compliance within 30 days are:

- 314.4(b)(2)—additional periodic risk assessments;[2]
- 314.4(d)(1)—regularly test or monitor effectiveness of the safeguards key controls, systems, or procedures;
- 314.4(f)(1) and (2)—overseeing service providers by: (1) taking reasonable steps to select and retain, and (2) requiring specific contract terms, and;
- 314.4(g)—Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d).

2 This is the only "new" requirement not expressly found in the current Rule.

Q Are there any exceptions?

A There is an exception to many of the new requirements within the Amended Rule for any entity that maintains 5,000 or fewer customer records. We believe that few, if any, dealers will be able to take advantage of this exception. However, dealers should consult with their vendors and professional advisors concerning this exception as well as the other aspects of the new requirements.

Q What about my OEM?

A There is no exception—and never has been—for your relationship with your OEM. Any programs you participate in, or services you obtain from your OEM, must comply with the requirements of the Safeguards Rule to the extent customer data is shared.

Q Will this be expensive for dealers?

A There is no clear answer to that question, but the new requirements are certainly extensive, complicated, and for many dealers will add significant costs. Note that during the time the FTC was considering the proposed rule, NADA submitted the results of an independent third-party cost study, conducted by an experienced IT services firm, that detailed the estimated costs to comply with many of the new requirements for the average sized dealership. A summary of that study is attached at Exhibit B. Importantly, several of the requirements outlined therein have been clarified or amended, or do not appear in the Amended Rule. We are hopeful that only a very few dealers will face all of these costs (as many dealers already meet some of the new requirements), and we certainly hope and expect that the market will provide efficiencies that do not exist today. However, that summary provides an estimate of what many dealers will be facing in terms of potential additional costs to comply with the Amended Rule.

Nothing in this FAQ document or the accompanying Exhibits is intended as legal advice. Dealers must consult with their attorney or other professional advisors regarding their own facts and circumstances, and application of the Amended Safeguards Rule to their operations. This document is only an overview of one federal regulatory requirement in this area and does not address state or local law in any way.

Suggested Steps to take – Now

- Determine your “qualified individual”
- Begin the data inventory process
- Notify/work with your vendors
  - Put them on notice that they must comply with new requirements
  - Many obligations apply to any third party with access to customer data
    - You must evaluate the security of any software
    - Including OEM and any OEM-vendors
  - Notify of new required contract provisions/duties
- Confirm/update compliance with current requirements

Suggested Steps to Take – Medium Term (2-4 mos)

- Complete Inventory
- WISP (updated)
- Written Incident Response Plan
- Implement technical requirements
  - E.g., Encryption / Dual factor authentication
- Create/Update other policies
  - Change management
  - “Board” reporting
  - Third-party audits

Suggested Steps to Take - By December 9, 2022

- Full compliance
  - Ensure all written policies in place
  - Complete all required training
  - Updated vendor review and contracts, including auditing provisions
    - If unable, obtain replacement vendor
  - All technical requirements tested and active
  - Create/Update all other policies and procedures

What is NADA Doing?

- FAQ Document
- Updated Driven Guide coming soon
- Additional all-member webinars coming soon
- Workshop at NADA 2022 Show
- Technical tools – stay tuned

Do you need third-party help?

- Its likely, but not required
  - Technical help
  - Third party IT audits
- Can rely on your vendors, but obligation is yours
- On the other hand – highly unlikely you can outsource everything
- Stay tuned from NADA…


Questions?


NADA