FTC STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

16 CFR PART 314

O'Connor & Drew P.C.
Certified Public Accountants

OCD TECH

MICHAEL HAMMOND, PRINCIPAL
mhammond@ocd.com
mhammond@ocd-tech.com

INTRODUCTIONS

- Michael Hammond
  - Principal, OCD Tech IT Audit & Security Services
  - 10 years at OCD, 15 at State Street Corp, 4 United States Air Force
  - mhammond@ocd-tech.com

- Kate Upton
  - Regulatory Specialist, OCD Tech, 3 years
  - Masters, Strategic Intelligence & Analysis
  - kupton@ocd-tech.com

WHAT IS THE FTC RULE?

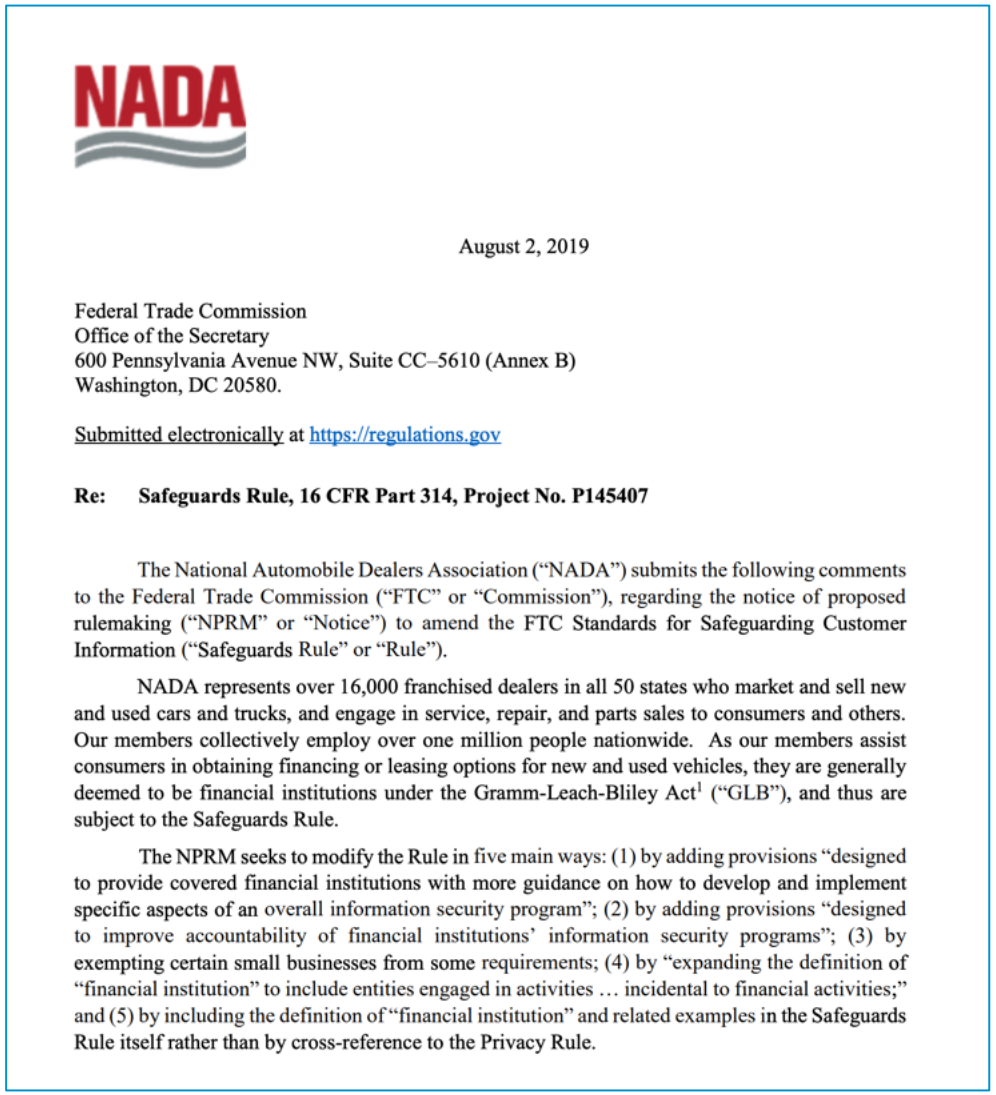
BACKGROUND
OCTOBER 27, 2021

THE SAFEGUARDS RULE WAS MANDATED BY CONGRESS UNDER THE 1999 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 lenders, **motor vehicle dealers**, and payday lenders, to **develop, implement,** and **maintain** a **comprehensive security system** to keep their customers' information safe.

NADA'S 49 PAGE COMMENT

BRADLEY MILLER
DIRECTOR, REGULATORY AFFAIRS
NATIONAL AUTOMOBILE DEALERS ASSOCIATION



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.

COST TO COMPLY

The National Automobile Dealers Association says small and midsize dealers will each have to spend hundreds of thousands of dollars initially and annually to comply with proposed changes to the FTC's Safeguards Rule. Here is NADA's step-by-step estimate:

	Small Dealer*		Midsize Dealer**	
Proposed change	One-time cost	Annual cost	One-time cost	Annual cost
Chief information security officer	$24,000	$42,000	$31,000	$60,000
Information security program based on written risk assessment	$20,500	$20,500	$32,500	$32,500
Data and systems inventory	$13,500	$9,000	$20,000	$11,500
Encrypt data at rest and in transit	$8,000	$8,000	$10,000	$9,000
Adopt secure development practices	$9,000	$37,500	$9,000	$37,500
Multifactor authentication for all accessing customer data	$17,500	$6,500	$50,000	$30,500
Include audit trails	$20,000	$12,000	$40,000	$24,000
Secure disposal procedure	$20,000	$3,600	$40,000	$18,000
Procedures for change management	$20,000	$2,000	$40,000	$2,000
Unauthorized activity monitoring	$15,000	$26,000	$25,000	$32,000
Penetration, vulnerability testing	$15,500	$17,500	$24,750	$28,750
Employee security awareness training	$1,400	$10,950	$2,800	$18,800
Periodic assessment of service providers	$12,000	$9,000	$16,500	$13,500
Required incident response plan	$16,000	$5,250	$16,000	$8,000
Required written chief information security officer report	$8,000	$8,000	$10,000	$10,000
Total cost incurred	$220,400	$217,800	$367,550	$336,050

*Operating on 1 site with roughly 50 employees
**Operating on as many as 5 sites with more than 50 employees
Source: NADA study

Automotive News
September 09, 2019 12:00 AM

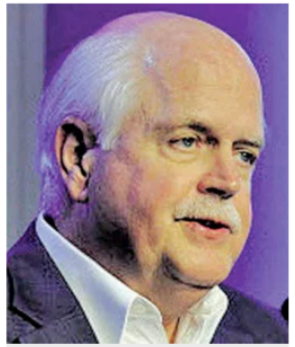
FTC's plan too costly to dealers, NADA says

Lindsay VanHulle Jackie Charniga

Proposed changes to the Federal Trade Commission's Safeguards Rule, which dictates how financial institutions safeguard consumer data, could add hundreds of thousands of dollars in costs to dealerships nationwide.

Potential revisions to federal data security rules could add billions of dollars in costs to U.S. auto dealerships in total, as stores already are slumped under the weight of shrinking margins and slowing new-vehicle sales.

Proposed changes to the Federal Trade Commission's Safeguards Rule, which dictates how financial institutions protect consumer data, would require dealerships nationwide to shell out hundreds of thousands of dollars each annually to comply, on top of what they spend to comply with other regulations, leaders of the National Automobile Dealers Association contend. NADA opposes the proposed changes and is asking the FTC to leave the rule as it is.



Welch: Smaller dealers will feel the squeeze.

"The numbers are staggering, even if we're off by 10 or 20 percent," NADA President Peter Welch told *Automotive News*.
The association estimates the total expense incurred by U.S. franchised dealerships could top $2.2 billion in initial startup costs, plus $2.1 billion per year in ongoing costs.

"It puts a squeeze particularly on our smaller dealers," Welch said.

In addition to higher costs for dealers, the proposed provisions may not even prevent some of the breaches, as intended, dealers and dealer advocates say. Lower compliance could be a consequence. But auto retailers' views aren't universally supported: Consumer advocates say any extra expenses should be the cost of doing business if that business includes financial transactions.

Safeguards Rule NPRM: Ex Parte Communication with NARA [NADA]

https://www.ftc.gov/system/files/documents/rules/safeguards-rule/safeguardsnprmexpartenada.pdf

United States of America
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

Office of Commissioner
Rohit Chopra

To: April Tabor

From: Maria Bazan

Date: September 15, 2020

Re: Safeguards Rule NPRM: Comments to be placed on the public record

---

On August 26, 2020, Commissioner Chopra, Erie Meyer, and I met via videoconference with representatives from the National Automobile Dealers Association (NADA) to discuss the Federal Trade Commission's Notice of Proposed Rulemaking regarding the Safeguards Rule.

During the meeting, Commissioner Chopra asked the NADA's representatives what constraints dealers face when implementing the information security and risk assessment measures required by the Safeguards Rule. They noted that choosing a service provider that both complies with the rule and is a good fit for their business can be a difficult task, because dealerships typically do not have much visibility into how these vendors operate and they are not able to easily oversee the dominant Dealer Management System (DMS) providers.

They also informed us that auto dealers are often limited in their ability to choose the service providers they use to store consumers' private information or the third parties they hire to audit their security protocols. In the case of franchise dealerships, it is common for car manufacturers to include terms requiring that dealers use specific vendors within their contracts. As a result, franchisees have a limited ability to switch service providers in the event of a data breach and, by extension, may not have the option to choose a more secure provider even if they did have visibility into their data protection measures.

Switching to a new vendor in order to comply with new minimum requirements of the rule could also be burdensome for independent dealerships given the costs of implementation. This is especially true for smaller, rural auto dealers who may not necessarily have the financial means to keep up with new technology. The NADA noted that approximately 37% of the NADA's 16,000 members sell less than 300 cars per year and many of their rural members have fewer than 15 employees. For a business of this size, options for affordable service providers may be more limited and the process of migrating their data to a new vendor might take a toll on the dealership's operating budget. The NADA suggested that a potential solution to this issue could be to implement a tiered system for enforcing the rule that takes into consideration the size of the business and the constraints they face when choosing a service provider.

DEAF EARS

PURPOSE OF THE UPDATED FTC SAFEGUARDS RULE

- This rule seeks to strengthen the data security safeguards that *financial institutions* have in place to protect customer data
- The FTC updated and finalized this rule to require non-banking financial institutions, such as auto dealers, mortgage lenders, and payday lenders to develop, implement, and maintain a comprehensive security system to safeguard consumer data

WHEN THE RULE COMES INTO EFFECT

- The federal rulemaking process involves the agency (such as the FTC) and the Federal Register through the National Archives
- The FTC has sent this final rule to the the National Archives to be published, and should be published **soon**

HOW THE RULE IS APPLIED

- The rule applies to *financial institutions* and has been expanded to include *finders*
- *Financial institutions* refer to mortgage lenders, **motor vehicle dealers**, and payday lenders.
- *Finders* refer to organizations that connect consumers with financial institutions, such as mortgage brokers or tax preparers

HOW THE RULE IS APPLIED, CONT.

- The rule applies to all financial institutions, regardless of size. However, if your organization holds data for fewer than **5,000 *consumers***, some requirements do not apply
- *Consumers* refers to individuals that act, "for personal, family, or household purposes". *Consumers* do not include businesses nor the employees therein that leverage your organization for services

EXCEPTIONS TO THE RULE

- For financial institutions that hold data for **fewer than 5,000 customers**, the following requirements do not apply:
  - Performing a risk assessment (314.4(b)(1))
  - Continuous monitoring or performance of penetration testing (314.4(d)(2))
  - Written incident response plan (314.4 (h))
  - Annual written update by the qualified individual for management (314.4(I))

WHAT CHANGED FROM THE PROPOSED RULE?

- From creating a new infosec program to comparing their existing program to the revised Rule, and address any gaps
- From Chief Information Security Officer (CISO) to designation of a single qualified individual. No particular level of education, experience, or certification is prescribed by the Rule, only that they be "qualified." A […] institution's coordinator [qualified individual] must have some level of information security training and knowledge

REQUIREMENTS FOR THE RULE

- Maintain a written InfoSec plan
- Designate a qualified individual
- Perform a risk assessment
- Periodically review access controls
- Manage data, personnel, devices, and facilities
- Use encryption at rest and in transit
- Maintain SDLC
- Actively manage MSPs
- Establish IR plan
- Implement MFA
- Maintain data retention policy
- Maintain change management process
- Monitor & log activity
- Continuous monitoring or pentest
- Maintain policies & procedures
- Establish security & awareness training
- Send a report, at least annually, to internal management on status for compliance

AM I COMPLIANT ALREADY? (NO ENDORSEMENT IMPLIED)

- Maintain a written InfoSec plan
  - Microsoft Word / Archer / HyperProof / ComplianceForge
- Designate a qualified individual
  - Internal or Outsourced. Must have training in information security, commensurate with the risk/size of the organization. **Does not need to be their only job**
- Perform a risk assessment
  - Microsoft Word / Archer / HyperProof / ComplianceForge
- Periodically review access controls
  - Internal or external auditors
- Manage data, personnel, devices, and facilities (Create and maintain an inventory)
  - Sharepoint / ServiceNow / Remedy / XLS

AM I COMPLIANT ALREADY? (NO ENDORSEMENT IMPLIED)

- Use encryption at rest and in transit (or use alternative means to protect customer information, subject to review and approval by the financial institution's Qualified Individual)
  - BitLocker / Sophos Endpoint / Websites with SSL
- Maintain SDLC (Not likely for auto dealers)
  - GitLab / Github
- Actively manage MSPs
  - SOC2 / SecurityScorecard / Venminder / Upguard / CyberGRX
- Establish IR plan
  - Microsoft Word / Policy

AM I COMPLIANT ALREADY? (NO ENDORSEMENT IMPLIED)

- Implement MFA
  - Microsoft MFA / Yubico / DUO
- Maintain data retention policy
  - Microsoft Word / Policy
- Maintain change management process
  - Microsoft Word / Policy
- Monitor & log activity
  - Sumologic / Splunk / AlienVault / Azure Sentinel
- Continuous monitoring or Pentest
  - Nessus / Qualys / Rapid7 / External Auditor

AM I COMPLIANT ALREADY? (NO ENDORSEMENT IMPLIED)

- Maintain policies & procedures
  - SharePoint / File share / Cabinet
- Establish security & awareness training
  - KnowBe4
- Send a report, at least annually, to internal management on status for compliance
  - Procedure

FTC CASE – ENFORCEMENT ACTIONS

- DealerBuilt
  - DealerBuilt stored information in clear text, without any access controls or authentication protections like passwords or tokens. Data transmitted between dealerships and DealerBuilt's backup database was in clear text, too.
  - DealerBuilt didn't have a written information security policy in place.
  - DealerBuilt didn't provide reasonable data security training for employees or contractors.
  - DealerBuilt didn't assess risks to the sensitive data on its network by conducting periodic risk assessments or performing vulnerability and penetration testing.
  - DealerBuilt didn't use readily available security measures to monitor – among other things – unauthorized attempts to transfer sensitive information.
  - DealerBuilt didn't put reasonable data access controls in place – for example, systems to limit inbound connections to known IP addresses or require authentication to access backup databases.
  - DealerBuilt didn't have a reasonable process to select, install, and secure devices with access to personal information.

FTC CASE – ENFORCEMENT ACTIONS

- **DealerBuilt**
  - The order requires a senior DealerBuilt officer to provide the FTC with annual certifications of compliance.
  - The order also requires DealerBuilt to implement specific, enforceable safeguards that address the issues alleged in the complaint – for example, requiring the company to conduct yearly employee training, monitor its systems for data security incidents, implement access controls, and inventory devices on its network.
  - In addition, the proposed order makes significant changes to further improve the accountability of a third-party assessor responsible for reviewing DealerBuilt's data security program.
  - What's more, the order gives the FTC increased access to documents and other materials upon which the assessor bases his or her conclusions.

FTC CASE – ENFORCEMENT ACTIONS

- IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years, unless otherwise specified below.

MASSACHUSETTS

MASS 201 CMR 17 (NOT A COMPLETE LIST, OVERLAP)

- Do you have a comprehensive, written information security program ("WISP") applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts ("PI")?
- Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices that contain personal information?
- Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- Have you evaluated the effectiveness of current safeguards?
- Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?

MASS 201 CMR 17 (NOT A COMPLETE LIST, OVERLAP)

- Does the WISP include policies and procedures for when and how records containing PI should be kept, accessed or transported off your business premises?
- Have you taken reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?
- Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?
- Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?
- Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?

MASS 201 CMR 17 (NOT A COMPLETE LIST, OVERLAP)

- Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?
- Do you, to the extent technically feasible, encrypt all PI stored on laptops or other portable devices?
- Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?
- Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?

CONNECTICUT

CT HB 6607, AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.

- HB 6607 **prevents** the Connecticut Superior Court from **assessing punitive damages** against an organization that **created, maintained and complied with a written cybersecurity program** that contains administrative, technical and physical safeguards for the protection of personal or restricted information, and that conforms to an industry-recognized cybersecurity framework (e.g., the Payment Card Industry Data Security Standard, the National Institute of Standards and Technology's Cybersecurity Framework, the ISO/IEC 27000-series information security standards).
- The safe harbor also applies in cases where the cybersecurity program conforms to applicable state or federal security laws and regulations (e.g., the security requirements of the Health Insurance Portability and Accountability Act and the **Gramm-Leach Bliley Act**).

CT HB 6607, AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.

- (ii) The National Institute of Standards and Technology's special publication 800-171;
- (iii) The National Institute of Standards and Technology's special publications 800-53 and 800-53a;
- (iv) The Federal Risk and Management Program's "FedRAMP Security Assessment Framework";
- (v) The Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense"; or
- (vi) The "ISO/IEC 27000-series" information security standards published by the International Organization for Standardization and the International Electrotechnical Commission.

REFERENCES

OCD Tech is the IT Audit & Security division of O'Connor & Drew P.C.

OCD Tech
25 Braintree Hill Office Park, Suite 102, Braintree MA, 02184
844-OCDTECH
617-472-7560
info@ocd-tech.com
https://ocd-tech.com

- https://www.ftc.gov/system/files/documents/federal_register_notices/2021/10/safeguards_rule_final.pdf
- https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial
- https://ocd-tech.com/it-audit-cybersecurity-services-bundle-for-auto-dealerships/