PUBLIC SUBMISSION

Comment Submitted by NADA

Posted by the **Federal Trade Commission** on Feb 7, 2022

View More Comments 21 (/document/FTC-2021-0071-0001/comment)

View Related Comments 21 (/docket/FTC-2021-0071/comments) Share

Comment

Attached please find comments from the National Automobile Dealers Association. Thank you.

Attachments 1

Safeguards_Proposed Notice Requirement_2_7_2022

Download (https://downloads.regulations.gov/FTC-2021-0071-0021/attachment_1.pdf)

Comment ID

FTC-2021-0071-0021

Tracking Number

kzd-bgxj-sn40

Comment Details **Submitter Info**

Received Date

Feb 7, 2022

Your Voice in Federal Decision Making

February 7, 2022

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 its proposal to further amend the Standards for Safeguarding Customer Information (''Safeguards Rule'' or ''Rule'') to require financial institutions to report to the Commission any security event where the financial institutions have determined misuse of customer information has occurred or is reasonably likely and at least 1,000 consumers have been affected or reasonably may be affected ("Proposed 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 1 million people nationwide. Most of our members are small businesses as defined by the Small Business Administration. Our members assist consumers in obtaining financing or leasing options for new and used vehicles and are generally deemed to be financial institutions under Gramm-Leach-Bliley, and thus are subject to the Safeguards Rule.

NADA opposes the requirement to notify the Commission about "any security event" because it is unnecessary, duplicative of similar duties under state law, and it ultimately does little to nothing to protect consumers or promote data security.

Proposed Section 314.4 would require financial institutions to:

> (*j) When you become aware of a security event, promptly determine the likelihood that customer information has been or will be misused. If you determine that misuse of customer information has occurred or is reasonably likely and that at least 1,000*

> *consumers have been affected or reasonably may be affected, you must notify the Federal Trade Commission as soon as possible, and no later than 30 days after discovery of the event. The notice shall be made electronically on a form to be located on the FTC's website, https://www.ftc.gov. The notice shall include the following:*
>
> *(1) The name and contact information of the reporting financial institution;*
>
> *(2) A description of the types of information that were involved in the security event;*
>
> *(3) If the information is possible to determine, the date or date range of the security event; and*
>
> *(4) A general description of the security event.*

I. The Proposed Reporting Obligation is Duplicative and Unnecessary

There are similar reporting obligations under state data breach laws. Even in those states that do not include a specific requirement to notify a state agency or attorney general, there is an obligation to notify all affected consumers. To the extent that the goal of this Proposed Rule is to ensure that consumers understand the security practices of financial institutions subject to the Rule, the Proposed Rule would be not only duplicative, but less effective as it does not directly notify a consumer.

The Proposed Rule notes this duplication, arguing that *"[t]o the extent state law already requires notification to consumers or state regulators [], there is little additional burden in providing notice to the Commission as well*."[1]

However, the scope of the duty under the Proposed Rule is unclear and at odds with many state data breach laws. For example, the Rule defines "Security Event" as: "*...an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form*."

This is broader that the general standard under state data breach notification laws, where "breach" is generally limited to "unauthorized access" to data stored in an electronic form containing personal information, not "disruption or misuse" of an information system.

Even if a financial institution can determine whether an "event" occurred, it may be difficult for financial institutions to know when such an event involved "customer information,"[2] and *then* to determine whether that information has been or is reasonably likely to be "misused." This will

[1] We disagree that notice under the Proposed Rule would be strictly duplicative for the reasons outlined herein, but even if it were, then one must ask why it is needed?

[2] This is especially true for automobile dealers who obtain and store consumer data of all types, only some of which contains nonpublic personal information, and thus "customer information." See NADA Comments to Safeguards Rule at p. 3. This makes the determination whether and how much "customer information" was involved in any particular security event a complicated and potentially difficult task.

require a separate analysis and given the vague and broad definition of "security event" this creates an additional burden, not outweighed by any consumer protection benefit.

Presumably, the determination of "likely misuse" will include questions about the nature of the data that was accessed and whether the data was encrypted – but that is also unclear. While the Commission declined to include encryption in its definition of "Security Event" in the Rule itself because they wanted financial institutions to undertake incident response steps even with respect to security events involving encrypted data,[3] that same justification does not exist in the context of the proposed notice requirement. And of course, the entire point of requiring encryption of the data is to prevent exposure that could be harmful to consumers, and any encryption that meets the requirements of the Rule will accomplish that task. Therefore, we would urge the Commission to adopt an explicit "carve-out" for encrypted data and clarify that the notification requirement applies only to: (a) the "unauthorized access" and (b) misuse or likely potential misuse of (c) *unencrypted* personal information.

Again, if its encrypted, it is not likely to be misused because it cannot be accessed, but without an explicit "carve-out" it could be a point of contention, and of course it would be another critical way that this obligation is an additional burden over state data breach regimes which generally apply to unencrypted data.

A. If Imposed, the Scope and Substance of The Notice Requirement Should Coincide With Existing Law.

While we do not agree that the Commission should impose a reporting requirement at all, if it does, we would urge the Commission to ensure that the scope of such reporting is defined and limited to any event where notice of data breach is provided under another current state or other federal law. This would ensure that financial institutions are not subject to differing or contradictory requirements, while ensuring that the Commission is notified in those states that do not require notice of a state agency. It would also avoid potential consumer confusion that would result from reporting incidents of differing scope and impact under state and federal law.

II. The Occurrence of a Data Breach Is Not a Proxy for Compliance with the Safeguards Rule and Reporting Breaches Will Not Promote Improved Data Security

Consumer notice, however, is not the stated purpose for the Proposed Rule. Instead, the purpose as noted in the Proposed Rule is to "*ensure the Commission is aware of security events that could suggest a financial institution's security program does not comply with the Rule's requirements, thus facilitating Commission enforcement of the Rule*."

But this simply does not follow. The occurrence of a "security event" at a financial institution is not a proxy for compliance with the Safeguards Rule. Of course, the standard under the Rule is "developing, implementing, and maintaining reasonable" safeguards to protect" customer

[3] See https://www.federalregister.gov/d/2021-25736/p-62

information, not guaranteed avoidance of security events. As noted in our comments to the Rule, there is nearly universal agreement that data breaches are impossible to prevent 100% of the time.[4] This is true regardless of the investment or effort put behind data security.[5] Financial institutions certainly do not want to suffer a data breach and when one occurs, they themselves are victims, along with their customers.[6] The notion that a security event should trigger an obligation to report because it "suggests" noncompliance with the Safeguards Rule would have the effect of imposing a de facto strict liability standard on financial institutions. That is not, and never has been the Rule.

While is logical to suggest that repeated data breaches may at some point be suggestive of compliance failures, certainly a single "event" is not. Indeed, compliance with the Rule requires constant monitoring and amendment of policies and procedures to address ongoing events and issues under a fully compliant program. At the very least, given the lack of connection between any security incident and Safeguards Rule compliance, the proposed reporting requirement should only apply after a series of security events, or similar events after notice.

In addition, even if a breach were in some way "suggestive" of compliance, we believe that a rule that requires financial institutions to self-report events in order to "facilitate" enforcement actions against themselves to be unprecedented. As noted above, state breach reporting requirements exist to promote consumer notice and protect against identity theft, not for enforcement of a regulation or the imposition of liability against the entity that suffered a breach. Even the other federal reporting requirements cited to in the notice[7] relate to the banking sector where the goal is

---

[4] 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

[5] 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). These firms, and others with similar outlays have nevertheless suffered breaches. See, e.g., https://www.wired.com/2015/11/four-indicted-in-massive-jp-morgan-chase-hack/

[6] 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;

[7] See Proposed Rule, fn 11. https://www.regulations.gov/document/FTC-2021-0071-0001

protection of prudential, institutional concerns about regulated industries, not to facilitate enforcement actions against victims of security events.[8]

The notion that a financial institution must report violations of a rule to its federal regulator - *for the specific purpose* of allowing that regulator to bring an enforcement action that could result in civil liability against the reporting entity raises serious questions.[9] We understand the conditional ("could suggest") manner in which this connection has been posed, but that does little to assure consumers or the financial institutions themselves that there is not a direct connection perceived by the Commission – especially given the stated tie to facilitating enforcement. Ultimately, we do not believe that such a requirement promulgated on this basis will promote security, only disincentivize reporting and sharing of security threats.

If data security is the goal, rather than forced self-reporting, we would suggest the promotion of threat intelligence and information sharing efforts that have proven successful in the financial services and other industries.[10] There are many existing information sharing and analysis centers, or ISACs that exist to allow competitors in a certain industry sector to share information about security threats in an antitrust compliant setting, and they have proved successful.[11] Efforts to share information about common threats, appropriate responses, and security tools and updates are critical and have proven beneficial to promoting data security. A regime that requires self-reporting at the specific threat of an enforcement action does not.

III. Any Information Reported to the FTC Should Remain Confidential

If a reporting obligation is imposed, any reports should remain confidential and should not be made public. The Proposed Rule asserts that making reported information public will "*assist consumers by providing information as to the security of their personal information in the hands of various financial institution*s." As noted above, this goal is duplicative of state law and potentially confusing to consumers – not only because the reported event may not be a "breach" under state law, but because the form of the information is different than the notice required under state law.

---

[8] Citations to banking regulator requirements to notify are inapposite as the purpose of banking regulation is to protect depositors and to ensure the public interest in the safety and soundness of banks. These concerns are not present for financial institutions like auto dealers. See, e.g., Banking Regulation: Its Purposes, Implementation, and Effects (kansascityfed.org) (stating that "Although banks are operated for profit and bankers are free to make many decisions in their daily operations, banking is commonly treated as a matter of public interest… The most basic reason for regulation of banking is depositor protection [as well as] a stable framework for making payments.")

[9] Including potential First Amendment and potentially even Fifth Amendment concerns given the potential not only for civil, but also criminal liability related to security events. (see, e.g., Uber ex-security chief faces additional charges of wire fraud – The Mercury News).

[10] See, e.g., https://www.nist.gov/publications/cyber-threat-intelligence-and-information-sharing

[11] For example, the Auto ISAC in the automotive space, the FS-ISAC in the Financial Services space, and many others.

The Proposed Rule also states the Commission's intention to "*input the information it receives from affected financial institutions into a database that it will update periodically and make available to the public*." And that "*the FTC does not believe the information to be provided to the Commission under the proposed reporting requirement will include confidential or proprietary information and, as a result, does not anticipate providing a mechanism for financial institutions to request confidential treatment of the information*."

We disagree that this information should be publicly available, particularly a "description of the security event." What data security benefit arises from a public database of affected financial institutions and a description of their specific security vulnerability? Public disclosure will do nothing to provide additional information to consumers, will not aid the Commission in enforcement efforts, but could instead highlight vulnerable financial institutions and provide a roadmap of common security weaknesses.

We would urge the Commission to consider instead maintaining the confidentiality of these reports, and using any information gleaned from such reports, along with its data security expertise to promote information sharing among financial institutions about cyber threats. Confidentiality is the cornerstone of all successful threat intelligence and information sharing. We do not believe there is any reason to make this information publicly available

IV. Specific Questions for Comment.

In addition to the comments above, here are brief responses to several of the specific questions that the Commission posed in the notice of the Proposed Rule:

(1) The information to be contained in any notice to the Commission. Is the proposed list of elements sufficient? Should there be additional information? Less?

A: We do not believe that there should be a reporting requirement, but if one is imposed, it should be limited to that information and those instances where notice is required under existing applicable state or federal law. In particular, the proposed requirement to include a "description of the security event" would be counterproductive at best.

(2) Whether the Commission's proposed threshold for requiring notice—for those security events for which misuse of the information of 1,000 or more consumers has occurred or is reasonably likely to occur—is the appropriate one. What about security events in which misuse is possible, but not likely?

A: As noted above, we would ask the Commission to consider clarifying that any such notice only applies to unencrypted data. We would also urge the Commission not to adopt a "possible" misuse standard as it would render the limitations virtually meaningless, since any event that meets the threshold could "possibly" lead to the misuse of the data. As the stated goal of this notice requirement is to facilitate enforcement actions against financial institutions, it should be at least tied to noncompliance with the Rule. The hallmark of the Safeguards Rule has been a reasonableness standard, not a mere *possibility* of misuse.

(5) **Whether the information reported to the Commission should be made public. Should the Commission permit affected financial institutions to request confidential treatment**

of the required information? If so, under what circumstances? Should affected financial institutions be allowed to request delaying the public publication of the security event information and, if so, on what basis?

A: We do not believe that such reports should be made public at all. As discussed above, there is no reason for public disclosure, and such a requirement would massively disincentive reporting and impact the analysis of whether any event should be reported, or any vulnerability shared with others so that they may protect themselves in the future.

(6) **Whether, instead of implementing a stand-alone reporting requirement, the Commission should only require notification to the Commission whenever a financial institution is required to provide notice of a security event or similar to a governmental entity under another state or Federal statute, rule, or regulation. How would such a provision affect the Commission's ability to enforce the Rule? Would such an approach affect the burden on financial institutions? Would such an approach generate consistent reporting due to differences in applicable laws?**

A; We believe that this approach makes the most sense by avoiding duplication, properly respecting the security of encrypted data, and providing the Commission with information without risking consumer confusion or public disclosure of security vulnerabilities.

(7) **Whether a notification requirement should be included at all.**

A: We do not believe so for the reasons stated above.

(8**) Whether notification to consumers, as well as to the Commission, should be required, and if so, under what circumstances.**

A: We do not believe that notification to consumers is required or helpful. Any such notice would be clearly duplicative with requirements that exist in all fifty states under state data breach laws. In addition, the receipt of a second, different notice related to the same breach/security event would likely raise additional questions for consumers, make them believe that another breach or event had occurred or otherwise confuse consumers more than enlighten them. There is also no connection between consumer notice and the GLB statutory mandate to the Commission related to data security. State data breach laws exist to protect consumers from potential identity theft related to a breach of their data. That is a laudable goal, but unrelated to the safeguarding of consumer data that provides the Commission's mandate under the Rule.

V. Conclusion.

Thank you for this opportunity to comment, and for your consideration of these views. We would welcome the opportunity to discuss these comments or any other related issues with the Commission at any time.

Sincerely,

/s/

Bradley Miller
Chief Regulatory Counsel, Digital Affairs and Privacy
National Automobile Dealers Association