PUBLIC SUBMISSION

Comment Submitted by AFSA - Celia Winslow

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

See attached file(s)

Attachments 1

AFSA Safeguards Comments FINAL Feb 2022

Download (https://downloads.regulations.gov/FTC-2021-0071-0012/attachment_1.pdf)

Comment ID

FTC-2021-0071-0012

Tracking Number

kzd-0yvt-mgl4

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 Ave NW, Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Standards for Safeguarding Customer Information
16 CFR Part 314, Project No. P145407

Dear Commissioners,

The American Financial Services Association (AFSA)[1] appreciates the opportunity to comment on the Federal Trade Commission's (FTC or Commission) supplemental notice of proposed rulemaking (NPRM) to further amend the Standards for Safeguarding Customer Information (Safeguards Rule or Rule). AFSA supports the FTC's efforts to protect customers' financial information in the wake of significant data breaches and cyberattacks in recent years. However, as we discuss in our comments, the proposed amendments to the reporting requirements of the Safeguards Rule are duplicative, unnecessary, and confusing. Below, we explain why another reporting requirement is unnecessary, where clarification is needed should the FTC proceed, and answer the questions the Commission poses in the supplemental notice.

I. Another Reporting Requirement will be Duplicative, Unnecessary, and Confusing

AFSA shares the FTC's goal of protecting consumers from the risks associated with a security breach, but the proposed rule would impose significant new requirements that could raise the cost of credit unnecessarily. The proposed requirements would create additional and unnecessary burdens, with little added consumer benefit, for data already protected by federal law and existing industry best practices.

II. Clarification Request

AFSA asks the FTC to clarify how it would use the incident reports it receives from financial institutions. In the proposed rulemaking, the FTC says the reporting would raise its awareness of "security events that suggest a financial institution's security program does not comply with the Rule's requirements," and thus help it enforce the Rule. But the FTC is not specific. Would the FTC investigate each one? Start an investigation after it received a certain number of incident reports? If so, how many?

The FTC gives no basis in the proposed rulemaking for the objective standards that might lead to an enforcement action resulting from the required report. If the FTC plans to use institutional reports as the basis for legal action to enforce the Rule, as compared to using them to inform future improvements to the Rule, then the FTC should clarify what factors in a report could lead to enforcement concerns. The proposed reporting requirement gives covered institutions no indication of when the submission of otherwise general information could trigger a deeper FTC review. This could render the proposed rule ineffective as institutions may seek to minimize all risks associated with a report since they will have little, if any, information about what the reporting risks for a given report might be.

[1] Founded in 1916, AFSA is the national trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including traditional installment loans, mortgages, direct and indirect vehicle financing, payment cards, and retail sales finance.

III. Answers to Specific Questions

(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?

The proposed information that the FTC already requests financial institutions furnish to the FTC is more than enough. However, if the FTC does require additional reporting, the FTC should explain what "customer information" is subject to the proposed rule and what data elements would trigger notification. Because of these uncertainties, a requirement to report to the FTC could conflict with the incident analysis and reporting parameters established by financial institutions that already comply with the standards promulgated by regulators akin to those required by the FTC. State data breach laws normally define exactly what personal information triggers a breach notification. AFSA asks the FTC to do the same or, better yet, give an exemption or safe harbor for institutions enforcing incident response plans in compliance with state laws.

Additionally, AFSA recommends that the FTC consider implementing a minimum standard for the sensitivity of information that is misused. For example, if a company loses 2,000 names only, would that require reporting? That information is much less sensitive and would pose less harm to consumers if misused than Social Security Numbers and personal addresses.

(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? Should there be a carve-out for security events solely involving encrypted data?

The 1,000-consumer record threshold is low considering the large number of financial institutions with many more customers. Large institutions have millions of accounts. Given the many protections in place for customer information, and the number of state requirements, the FTC should raise the threshold to reduce the regulatory burden on financial institutions. As for security events in which "misuse is possible, but not likely," AFSA asks the FTC to clarify what this means versus "likelihood of harm," a phrase which the FTC used as it sought input in the NPRM.

Additionally, security events should not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable. As such, AFSA recommends a carve-out for security events solely involving encrypted data (unless the key is also disclosed) in alignment with state laws which handle encrypted data differently. For example, in Texas, security breaches are defined as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."[2] And in Florida, the definition of personal information "does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable."[3]

(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?

The information reported to the Commission should *not* be made public. Financial institutions should be allowed to ask that required information given to the FTC about security events stay confidential. The FTC says making reports publicly available would "assist consumers by providing information as to the security of their personal information

[2] Tex. Bus. & Com. §521.03 (2001) https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm#521.053.
[3] Fla. Stat. § 501.171 (2014) https://www.flsenate.gov/laws/statutes/2014/501.171.

in the hands of various financial institutions." But the level of information an institution would have to report, which the FTC appropriately proposes to keep at a high level to avoid placing excessive burden on institutions, would be too general to be useful to an individual consumer. And such general reports could trigger unnecessary media coverage that could raise unwarranted concerns for consumers.

(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?

Although AFSA agrees that it is important to report data breaches and misuse of consumer information, existing state data breach laws already require financial institutions to notify customers about data breaches. Requiring institutions to also report to the FTC would give consumers no real additional benefit.

If financial institutions must report misuses of customer information to the FTC, this reporting should preempt state reporting for the same event. Alternatively, it would be more appropriate for the FTC to postpone this rulemaking until Congress addresses preemption and makes the federal reporting requirement preempt state laws.

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

A notification requirement is unnecessary. As explained above, financial institutions already have reporting requirements under state law. We further note states regularly update law relating to data breach notification. For example, there are pending bills in Arizona, Idaho, Illinois, Indiana, Minnesota, New Jersey, New York, Pennsylvania, Tennessee, and West Virginia—with more likely to be introduced as states convene for the 2022 legislative sessions. We believe this shows the states are fulfilling the role this rulemaking seeks to accomplish on the federal level.

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

There is no need for a notification requirement to consumers. First, one already exists. And second, adding many reports to consumers will be overwhelming and might lead consumers to ignore them.

* * *

AFSA appreciates your attention to these important issues. If you have any questions or require additional information, please do not hesitate to contact me at 202-776-7300 or cwinslow@afsamail.org

Sincerely,

Celia Winslow
Senior Vice President
American Financial Services Association