U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF ADVOCACY
REGULATION • RESEARCH • OUTREACH

July 31, 2019

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

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

Dear Commissioners:

The Office of Advocacy of the U.S. Small Business Administration (Advocacy) submits these comments on Federal Trade Commission's (FTC) notice of proposed rulemaking (NPRM) on *Standards for Safeguarding Customer Information*.[1] The FTC is proposing to modify its current Standards for Safeguarding Customer Information by adding provisions and expanding the definition of "financial institution." Advocacy is concerned that the FTC may not fully understand the potential economic impact of this rulemaking on small entities. Advocacy encourages the FTC to maintain the status quo for small entities until it has the data to access fully the potential economic impact on small entities.

Advocacy Background

Advocacy was established pursuant to Pub. L. 94-305 to represent the views of small entities before federal agencies and Congress. Advocacy is an independent office within the U.S. Small Business Administration (SBA), so the views expressed by Advocacy do not necessarily reflect the views of the SBA or the Administration. The Regulatory Flexibility Act (RFA),[2] as amended by the Small Business Regulatory Enforcement Fairness Act,[3] gives small entities a voice in the rulemaking process. For all rules that are expected to have a significant economic impact on a

[1] 84 Federal Register 13158, April 4, 2019.
[2] 5 U.S.C. § 601 et seq.
[3] Pub. L. 104-121, Title II, 110 Stat. 857 (1996) (codified in various sections of 5 U.S.C. § 601 et seq.).

substantial number of small entities, federal agencies are required by the RFA to assess the impact of the proposed rule on small business and to consider less burdensome alternatives.

The Small Business Jobs Act of 2010 requires agencies to give every appropriate consideration to comments provided by Advocacy.[4] The agency must include, in any explanation or discussion accompanying the final rule's publication in the Federal Register, the agency's response to written comments submitted by Advocacy on the proposed rule, unless the agency certifies that the public interest is not served by doing so.[5]

The Office of Advocacy performs outreach through roundtables, conference calls and other means to develop its position on important issues such as this one. Advocacy held a roundtable on the Safeguards Rule and spoke with trade associations about the proposed rule.

The Existing Rule

In May 2003, the FTC implemented the Safeguards Rule pursuant to the Gramm Leach Bliley Act. The Safeguards Rule requires a financial institution to develop, implement, and maintain a comprehensive information security program that consists of the administrative, technical, and physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. The information security program must be written in one or more readily accessible parts. The safeguards set forth in the program must be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue. The safeguards must also be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. [6]

In order to develop, implement, and maintain its information security program, a financial institution must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. The financial institution must then design and implement safeguards to control the risks identified through the risk assessment and must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures. The financial institution is also required to evaluate and adjust its information security program in light of the results of this testing and monitoring, as well as any material changes in its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program. The financial institution must also designate an employee or employees to coordinate the information security program.[7]

Finally, the Safeguards Rule requires financial institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer

[4] Small Business Jobs Act of 2010 (PL 111-240) § 1601.
[5] Id.
[6] 84 Fed. Reg. at 13158-13159.
[7] Id.

information and require those service providers by contract to implement and maintain such safeguards.[8]

The Proposed Rule

On April 4, 2019, the FTC published the NPRM on Standards for Safeguarding Customer Information ("Safeguards Rule"). The proposal contains five main modifications to the existing rule. First, it adds provisions designed to provide covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program. Second, it adds provisions designed to improve the accountability of financial institutions' information security programs. Third, it exempts small businesses from certain requirements. Fourth, it expands the definition of "financial institution" to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities. Finally, the Commission proposes to include the definition of "financial institution" and related examples in the rule itself rather than cross-reference them from a related FTC rule, the Privacy of Consumer Financial Information Rule.[9]

Advocacy Is Concerned that FTC's IRFA Lacks Required Information

When an agency issues an NPRM, it is required to perform an initial regulatory flexibility analysis (IRFA) unless it can certify that the proposed rule will not have a significant economic impact on a substantial number of small entities.[10] The FTC prepared an IRFA for the NPRM but also stated that it does not believe the rule, if adopted, will have the threshold impact on small entities.[11]

While Advocacy appreciates the fact that the FTC prepared an IRFA for the NPRM and requested information from the public, Advocacy is concerned that the IRFA lacks sufficient data. To comply with the RFA, an agency must examine costs and other economic implications for the industry sectors targeted by the rule. Impacts include costs of compliance and economic implications that derive from additional compliance costs such as economic viability (including closure), competitiveness, productivity, and employment. The analysis should identify cost burdens for the industry sector and for the individual small entities affected.[12] The analysis should also contain description of the small entities that may be impacted by the proposal[13] and a description of significant alternatives.[14]

It is important to note that that Section 603 (c) requires an agency to provide a description of alternatives which accomplish the stated objectives of the applicable statutes and which minimize any significant economic impact of the proposed rule on small entities. An agency

[8] Id.
[9] 84 Fed. Reg. at 13158.
[10] See, 5 USC §605 (b).
[11] 84 Fed. Reg. at 13172.
[12] *A Guide for Federal Agencies: How to Comply with the Regulatory Flexibility Act*, page 32.
[13] See, 5 USC §603 (b).
[14] See, 5 USC §603 (c).

cannot consider alternatives that minimize any significant economic impact if the agency does not know what the economic impact of the proposed action is.

In the NPRM, the FTC requests, but does not provide, data about the costs of the NPRM for small entities to comply and the costs to the newly covered financial institutions (finders) of establishing and operating an information security program[15] as required by Section 603 of the RFA. The FTC also stated that it was not feasible to determine the precise estimate of the number of small entities. However, it acknowledges that the rule covers financial institutions, lenders, financial advisers, collection agencies, financial advisers, tax preparers, and real estate settlement services to the extent that they have customer information.[16] The discussion of alternatives in the IRFA was limited to design standards and an exemption for some small businesses. The FTC published the IRFA and invited comment on the potential impact on small entities.

The Rule Is Much More Prescriptive than It Needs to Be

Advocacy contacted trade associations that represent small entities about this issue. The trade associations told Advocacy that the proposal is overly prescriptive and creates a high burden for small entities without any data on how it will lower risks to consumers. They also stated that the changes impose national bank data security standards on companies with only a few offices. Moreover, some of the changes include protecting additional information (not just sensitive information), increased encryption levels, increased storage/server ability, creating a different way to access information, creating new audit trails, purging software systems in a new manner, and increase internal audits and staff to do the additional work. These are expensive requirements that will be burdensome to small entities.

They further stated that some of the requirements, like having a chief information security officer, may be nonsensical for small entities because the businesses only have a few employees. They are also concerned about the expansion of the definition of small entities to include "finders", a group that has not been a part of the rule in the past, and the impact that the proposal may have on third party vendors.

Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson voiced similar concerns in their dissent to this action. They stated:

> "…the Safeguards Rule today is a flexible approach, appropriate to a company's size and complexity. This proposal would move us away from that approach. There are direct costs for enhanced precautions, but this record does not demonstrate that those costs will significantly reduce data security risks or significantly increase consumer benefits. The expansion of the Rule could create traps for the unwary, especially small and innovative businesses. Further, large incumbents can often absorb regulatory compliance costs more effectively than new entrants or smaller players, potentially decreasing competition. The proposed precautions, either individually or in the aggregate, may constitute best practices for certain firms. But the proliferation of procedural, technical, and governance

[15] 84 Fed. Reg. 13173
[16] 84 Fed. Reg. at 13172.

> requirements may have the unintended consequence of diluting core data security measures undertaken pursuant to the existing Safeguards Rule."[17]

The dissenting Commissioners also state that the proposed rule is based in substantial part on regulations promulgated two years ago by the New York State Department of Financial Services. They argue that the FTC does not have data about the impact and efficacy of those regulation, so whether to adopt a version of them at the federal level and whether that version should be a floor for or should preempt state-level rules seem like questions worthy of more study.[18]

Advocacy agrees with Commissioners Phillips and Wilson. Waiting for data would allow the FTC to be able to thoroughly assess the impact of this action on small entities. If the FTC waits, it will be able to gather data and extrapolate the potential impact that a similar federal proposal may have on small entities, allowing the agency to fill in the blanks that now exist in the rule's RFA analysis. As noted above, small entities believe that this matter will be extremely burdensome. Allowing for time to assess the impact is the prudent course of action.

Maintaining the Status Quo is a Viable Alternative for Small Entities Until the FTC Can Pursue a More Viable Strategy

In the discussion of the alternatives, the FTC states that it is introducing design standards (e.g. a company must implement encryption, authentication, incident response) in addition to the performance standards (reasonable security) that are currently in place. The FTC acknowledges that the design standards may introduce additional burden but states that it believes the burden will be minimal. The FTC provides no basis for the statement that the burden will be minimal. There is also no explanation as to how adding a requirement that will impose an additional burden is a significant alternative for reducing the burden on small entities.[19]

The FTC also states that it is exempting small entities that maintain relatively small amounts of customer information from certain requirements of the amended Safeguards Rule. The exemption applies to financial institutions that maintain customer information for fewer than five thousand customers. The institutions that qualify for the exemption would not have to perform a written risk assessment, conduct continuous monitoring or annual penetration testing and biannual vulnerability assessment, prepare a written incident response plan, or prepare and annual written report by the Chief Information Security Officer. Exempted institutions will still be required to conduct risk assessments, design and implement a written information security program with the required elements, utilize qualified information security personnel and train employee, monitor activity of authorized users, oversee service providers, and evaluate and adjust their information security programs. [20]

---

[17] Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson, Regulatory Review of Safeguards Rule Matter No. P145407, March 5, 2019, page 2.

[18] Id.

[19] 84 Federal Register at 13173

[20] Id.

While Advocacy appreciates the fact that the FTC has exempted some small entities from a portion of the proposed rule, Advocacy is concerned that the proposal will be unduly burdensome for small entities. Too little is known about the potential impact of this proposal at this time. If it is unduly burdensome, it may result in small entities having to leave the marketplace. The best alternative for assuring that the action will not be unduly burdensome is to maintain the status quo for small entities, as defined by the SBA size standards, until FTC can ascertain the potential impact an pursue a more viable strategy.

Conclusion

The RFA establishes a principle of regulatory issuance that agencies shall endeavor, consistent with the rules and of applicable statutes, to fit regulatory and informational requirements to the scale of the businesses, organizations, and governmental jurisdictions subject to regulation. In this instance, the proposal would impose stringent requirements on small entities without the FTC knowing what the impact may be. It may force some small entities to exit the market, which could impede competition. Advocacy implores the FTC to maintain the status quo for small entities until the FTC can ascertain the quantitative impact on small entities.

Thank you for the opportunity to comment on this important proposal and for your consideration of Advocacy's comments. If you have any questions regarding these comments or if Advocacy can be of any assistance, please do not hesitate to contact me or Jennifer Smith at (202) 205-6943.

Sincerely,

/s/
Major L. Clark, III
Acting Chief Counsel
Office of Advocacy
U.S. Small Business Administration

/s/
Jennifer A. Smith
Assistant Chief Counsel
For Economic Regulation & Banking
Office of Advocacy
U.S. Small Business Administration