Before the
FEDERAL TRADE COMMISSION
Washington, DC

In the Matter of	)	
	)	
Notice of Proposed Rulemaking Concerning the Safeguards Rule	)	Project No. P145407
	)	
	)	
16 CFR PART 314	)	

COMMENTS OF ACA INTERNATIONAL

Leah Dempsey
Vice President and Senior Counsel, Federal Advocacy
ACA International
509 2nd St., NE
Washington, DC 20002

Before the
FEDERAL TRADE COMMISSION
Washington, DC

In the Matter of	)	
	)	
Notice of Proposed Rulemaking Concerning the Safeguards Rule	)	Project No. P145407
	)	
	)	
16 CFR PART 314	)	

COMMENTS OF ACA INTERNATIONAL

I. Introduction.

ACA International ("ACA") files these comments in response to the Federal Trade Commission's ("FTC" or "Commission") request for comments concerning proposed amendments ("Proposed Amendments") to the Standards for Safeguarding Customer Information (''Safeguards Rule'' or ''Rule''),[1] as published in its Notice of Proposed Rulemaking ("NPRM") in the Federal Register on April 4, 2019.[2]

Most ACA members are considered "financial institutions" subject to the Safeguards Rule because they collect consumer debt. These organizations would incur the costs to comply with the Proposed Amendments.

The current Safeguards Rule provides a sufficient data security framework to accomplish the Commission's data security goals. ACA and its members understand the importance of reasonable data security practices, and members already devote significant resources to data security programs. As discussed in more detail below, amending the Safeguards Rule would unnecessarily raise costs on ACA members and other financial institutions without a material benefit to consumers or information security. To the extent that the Commission nonetheless advances the Proposed Amendments, it should revise certain proposals to avoid unnecessarily burdening financial institutions while continuing to protect consumers.

---

1 16 C.F.R. § 314 (2019).
2 84 Fed. Reg. 13,158 (Apr. 4, 2019).

A. Overview of ACA International.

ACA International was originally formed in 1939 and is the largest trade group for the debt collection industry, representing approximately 2,500 members, including credit grantors, third-party collection agencies, asset buyers, attorneys, and vendor affiliates.[3] Collectively, ACA members employ more than 129,000 individuals worldwide.[4] ACA members range in size from small businesses with a few employees that operate within a limited geographic range of a single state to large, multinational corporations that operate in every state.[5]

The majority of ACA members are small businesses. ACA member organizational demographics are as follows:

- 44% of ACA member organizations (831companies) have fewer than nine employees.
- 85% of ACA member organizations (1,624 companies) have 49 or fewer employees.
- 93% of ACA member organizations (1,784 companies) have 99 or fewer employees.[6]

ACA members provide businesses with an effective way of recovering outstanding payments. ACA members recover and return billions of dollars each year to local, national, and multinational companies that provide consumer goods and services. Without our members, businesses could suffer significant economic losses that would threaten their economic viability and, in turn, the health of the American economy. By way of illustration, in 2016, third-party collection agencies recovered approximately $78.5 billion in total debt and returned $67.6 billion to creditors.[7] This return to creditors represents an average savings of $579 per household, as businesses were not compelled to compensate for lost capital through increased prices.[8]

ACA members obtain consumer information for legitimate business reasons to facilitate monetary recovery for their clients across industries. Consequently, ACA members are subject to a

---

[3] ACA International Fact Sheet, January 2019, https://www.acainternational.org/assets/advocacy-resources/aca-fact-sheet.pdf?viawrapper (last visited August 1, 2019).

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

myriad of federal and state consumer protection laws and regulations. Depending on the type of accounts subject to collection, these laws and regulations can include the Federal Trade Commission Act,[9] the Fair Debt Collection Practices Act,[10] the Fair Credit Reporting Act,[11] and the Health Insurance Portability and Accountability Act of 1996,[12] among others. As ACA members, they are also bound to the ethical standards and guidelines established by ACA.

II. The Proposed Amendments are Not Necessary at this Time.

The Proposed Amendments are not necessary at this time to protect consumers. For nearly twenty years, the current Safeguards Rule has provided the Commission with a robust, flexible tool to protect consumers. The Commission has presented no concrete evidence to demonstrate that the Safeguards Rule is inadequate or needs changing. As discussed further below: (A) the Safeguards Rule provides a sufficient framework to regulate covered financial institutions' information security programs; (B) the Proposed Amendments are more stringent than necessary to achieve the Rule's objectives; (C) the Proposed Amendments could stifle innovation and handicap small businesses; and (D) the Proposed Amendments are premature.

A. The Safeguards Rule Remains Sufficient to Protect Consumers.

The longstanding framework of the Safeguards Rule is flexible yet robust. It is appropriately risk-based, requiring financial institutions to assess their information security risks and to design and maintain an information security program with safeguards "appropriate to [their] size and complexity, the nature of [their] activities, and the sensitivity of the customer information" they possess.[13] The Safeguards Rule sets forth components that are central to an adequate information security program, such as designating one or more employees to coordinate the program, setting the areas of consideration required for adequate risk-assessments, requiring periodic monitoring and testing of

9 15 U.S.C. § 45 *et seq.*
10 15 U.S.C. § 1692 *et seq.*
11 15 U.S.C. § 1681 *et seq.*
12 42 U.S.C. § 1320d-2.
13 16 C.F.R. § 314.3(a).

the program, and mandating service provider oversight. Yet, it also provides a covered financial institution with sufficient flexibility to determine the means by which it achieves these objectives.

The Commission seems to be concerned with the Safeguards Rule keeping pace with evolving security threats.[14] But the Safeguards Rule already accounts for evolving expectations of reasonable security, with appropriate consequences for non-compliance. In 2002, the FTC aptly endorsed its Safeguards Rule, concluding that it struck "an appropriate balance between allowing flexibility to financial institutions and establishing standards for safeguarding customer information that are consistent with the Act's goals."[15] Where the Commission believes that a financial institution subject to its jurisdiction has not employed reasonable security, the Commission has a basis to enforce against those companies, which it has done repeatedly.[16] The Commission's Safeguards Rule enforcement actions have reflected evolving security standards and continue to convey important signals about reasonable security.[17]

The Commission also has other tools besides amending the Safeguards Rule to convey messages about its expectations for financial institutions regarding reasonable data security. In 2002 upon issuing the final Safeguards Rule, the Commission also stated that it would "issue educational materials in connection with the Rule [to] assist businesses . . . to comply with its requirements without imposing undue burdens."[18] The Commission has done so periodically, and

---

[14] 84 Fed. Reg. 13,160 (Apr. 4, 2019) (Discussing that the purpose of the Proposed Amendments is to enable covered financial institutions to "respond to the changing landscape of security threats . . .").

[15] Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (May 23, 2002).

[16] *See e.g.*, Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm'n v. Equifax, Inc., No. 19-cv-03297-TWT (N.D. Ga. July 23, 2019), ECF No. 6, https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf; Agreement Containing Consent Order, In the Matter of Paypal, Inc., No. 162-3102, https://www.ftc.gov/system/files/documents/cases/venmo_agreement_with_decision.pdf; Decision and Order, In the Matter of TaxSlayer, LLC, No. C-4626: https://www.ftc.gov/system/files/documents/cases/1623063_taxslayer_decision_and_order.pdf; Agreement Containing Consent Order, In the Matter of Lightyear Dealer Techs.,, LLC, https://www.ftc.gov/system/files/documents/cases/172_3051_dealerbuilt_final_consent_agreement_6-12-19.pdf.

[17] *See e.g.*, Complaint, In the Matter of Taxslayer, LLC, No. C-4626 (Oct. 20, 2017), https://www.ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_decision_and_order.pdf (inferring inadequate security based in part on a lack of multi-factor authentication, a requirement not stated in the Rule).

[18] Standards for Safeguarding Customer Information, 67 Fed. Reg. 36,484 (May 23, 2002).

such guidance has provided an important message to financial institutions about reasonable data security practices.[19] In addition, the Commission's guidance regarding data security practices as enforced under Section 5 of the FTC Act, for which the Commission uses a "reasonableness" standard, also serves to inform the business community at large, including Commission-regulated financial institutions, about evolving security expectations.[20] Commissioner and agency speeches and writings can also be instructive.[21]

B. The Proposed Amendments are More Stringent than Necessary to Protect Consumers.

The Commission cites no evidence that the current Safeguards Rule is insufficient or not working well. The FTC itself has acknowledged that no parties have perfect security measures,[22] and although there have been some covered financial institutions that have had security shortcomings in recent years, the number of incidents remains relatively low. Moreover, as noted above, where the Commission has deemed the practices unreasonable, it has the ability to, and has,

---

[19] Financial Institutions and Customer Information: Complying with the Safeguards Rule, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (April 2006) (last visited August 1, 2019).

[20] *See,* Start with Security, A Guide for Business, Lessons Learned from FTC Cases, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf. For a continuing series of blog posts that build on this guidance, see Thomas B. Pahl, *Stick with Security: Insights into FTC Investigations*, FTC Bureau of Consumer Protection (July 21, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations.

[21] *Protecting Consumers' Data: Policy Issues Raised by Choicepoint: Hearing Before H. Subcommittee on Commerce, Trade, and Consumer Protection Committee on Energy and Commerce* (2005) (statement of Federal Trade Commission), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-subcommittee-commerce-trade-and-consumer-protection/050315protectingconsumerdata.pdf; *Consumer Privacy: Hearing Before the S. Committee on Commerce, Science, and Transportation* (2010) (statement of Federal Trade Commission), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy/100727consumerprivacy.pdf.

[22] *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), at 1, *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf ("Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.").

brought enforcement actions against those companies. The FTC has not indicated, however, that an industrywide gap exists that warrants expanding the current Safeguards Rule.

In addition, the requirements that would be added by the Proposed Amendments would not necessarily reduce the risk of consumer information being exposed and could actually *increase* such risk. For example, a covered financial institution may end up replacing a well-tailored, meaningful, information security program with a more standardized, check-the-box program that is designed to simply meet the mandates of the Proposed Amendments. In that respect, the Commission's adoption of the Proposed Amendments could add considerable stringency without contributing to the underlying consumer protection objectives.

One example is the proposed section 314.4(a), requiring covered institutions to "designate a qualified individual responsible for overseeing and implementing …and enforcing [the institution's] information security program (for purposes of this part, 'Chief Information Security Officer' or 'CISO'"). The current Safeguards Rule already requires institutions to "[d]esignate an employee or employees to maintain [its] information security program."[23]

The CISO requirement is too rigid and burdensome without a clear benefit to consumers. In the Supplementary Information to the Proposed Amendments, the FTC indicates that the CISO requirement is designed to ensure that there are no gaps in responsibility or accountability between responsible individuals. However, ensuring responsibility and accountability across a financial institution's broader information security program does not *require* a CISO and can be met through the current Safeguards Rule. The current Rule requires an employee or employees to lead the program, inherently suggesting they have some reasonable level of competence (that, if lacking, the Commission could view as unreasonable). Many ACA members have CISOs, but some have developed alternative approaches that are still led by an employee or sometimes two or more that team together to have responsibilities over their information security program. There is also no evidence cited by the Commission in the NRPMsuggesting that oversight for an information security

[23] 16 C.F.R. § 314.4(a) (2019).

program that is shared by a team is necessarily substandard to one led by or accountable to a single individual.

C. The Proposed Amendments Could Stifle Innovation and Handicap Small Businesses.

As noted in Section I above, many ACA members are small businesses. The Proposed Amendments are a sweeping overhaul of the current framework upon which ACA members have relied in developing their information security programs. As mandated by the current Safeguards Rule, ACA members already devote resources to "develop, implement, and maintain" comprehensive information security programs that are appropriately designed for their businesses and the consumer information that they collect. The Proposed Amendments add a number of costly administrative and technical controls to these obligations for covered financial institutions without clear benefit to consumers.

Returning to the CISO example raised in the subsection above, even though the Commission acknowledges that the title would not be technically required, the requirement of a CISO also places an undue burden on small financial institutions, as for them even one additional hire of any employee can have a significant economic impact. The demand for CISOs is already extremely high, in part due to regulatory requirements in certain states. Adding the CISO (or CISO-like) requirement to the Safeguards Rule will only add to that demand and further drive up costs, making the position highly impractical for small businesses. These and other costs imposed by the Proposed Amendments could also reduce competition (given the impact on small businesses and new entrants). The Commission, expressly motivated by recent regulatory and legislative activity in a small number of states,[24] is at risk of elevating form over substance; financial institutions may need

[24] Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500, *et seq.* (2016) [hereinafter "NYDFS Rule"]; S. 273, ORC §§3965.01-11, 133rd Gen'l Assembly (Oh. 2019); H.R. 6491, MCL §500.550 (Mich. 2018); S.C. Code Ann. § 38-99-10, *et seq.* (2019), https://www.scstatehouse.gov/code/t38c099.php; *see* Harriet Pearson, Timothy Tobin and Morgan Perna, *Cybersecurity Standards for the Insurance Sector – A New Patchwork Quilt in the US?,* Cybersecurity and Data Breaches (May 13, 2019), https://www.hldataprotection.com/2019/05/articles/cybersecurity-data-breaches/cybersecurity-standards-for-the-insurance-sector-a-new-patchwork-quilt-in-the-us/ (background).

to replace or significantly change existing, effective information security programs with programs to merely meet the requirements of the Proposed Amendments.

The Commission's reliance on a small number of states that have acted to further regulate the requirements of specific licensed entities in those states also alters the options that ACA members have had as a result of those regulations. Only one of those states' regulations, New York, through its Cybersecurity Rule, could apply to some ACA members.[25] Some potentially impacted ACA members could simply exit the purview of the NYDFS Rule by removing their covered business from the licensing requirements of the State of New York. As challenging of a decision as that may have been for some ACA members, it was a viable option, but is not something the Proposed Amendments allow. If enacted, the only congruent option afforded by the Proposed Amendments would be for smaller ACA members to exit the U.S. debt collection market altogether. As a result, the market – and the clients served by ACA members – would suffer.

D. The Proposed Amendments are Premature.

The Commission states that the Proposed Amendments "are based primarily on the cybersecurity regulations issued by the New York Department of Financial Services … and the insurance data security model law issued by the National Association of Insurance Commissioners [(NAIC)]."[26] Although it is understandable that the Commission could be concerned about perceptions that these bodies are moving ahead of it on data security regulation, it should not succumb to the pressure to change an already effective regime for unproven approaches, especially given the burdens and costs on financial institutions. The NYDFS Rule did not become fully effective until February 28, 2018, less than two years ago. And although NAIC passed its model code in 2017, to date, only three states, Michigan, Ohio and South Carolina, have passed implementing legislation or regulations. It is not yet known whether these new laws and regulations are offering consumers an appreciably significant benefit in terms of enhanced data security, especially in light of the added costs to businesses. It does not make sense to rush to make

25 The other three states' regulations apply to the business of insurance.
26 84 Fed. Reg. 13,163 (Apr. 4, 2019).

changes to a longstanding, robust regime without a better understanding of the full impact of the NYDFS and NAIC frameworks.

In addition, Congress has been considering various options for new federal legislation that could affect or alter the Safeguards Rule.[27] The FTC has regularly been providing its perspective to Congress on approaches to data security regulation and enforcement. Given the weight, importance, and urgency of the concerns at issue, ACA urges the Commission to abstain from rulemaking until more comprehensive approaches to privacy and data security can be fully explored by Congress.

III. If the FTC Proceeds with the Proposed Amendments, it Should Modify Key Aspects of the Proposals.

To the extent that the Commission nonetheless moves forward with amending the Security Rule, several of the Proposed Amendments could be unnecessarily burdensome for financial institutions and should be revised.

A. The section 314.5 effective date should be prolonged.

If the Commission amends the Safeguards Rule, it should consider a minimum one-year effective date for the various requirements. Given the breadth of the administrative and technical requirements in the Proposed Amendments, ACA also strongly recommends the FTC consider adding an additional, temporary good-faith compliance period for covered financial institutions.

Section 314.5 of the Proposed Amendments provides six months after the publication of the final rule for implementation of the changes. Many of the changes in the Proposed Amendments would require financial institutions to make changes that, even with best efforts, will take longer than six months to implement. The timing is especially problematic for many ACA members, who may not meet the Commission's small business criteria as set forth in the NPRM but are nonetheless objectively small in terms of the burdens that a new Security Rule would impose. By way of illustration, a covered financial institution that complies with the Safeguards Rule, but is not covered by the NYDFS Rule or a similar framework, may not have a CISO. It also may not have

[27] 84 Fed. Reg. 13,170 - 13,173 (Apr. 4, 2019).

implemented the technical measures imposed by the Proposed Amendments. Assuming that the entity is able to quickly divert its budgetary resources to hire a CISO or someone with that function, actually finding and hiring someone with the relevant qualifications could take months. Implementing technical measures can also take time to roll out across an organization.

A six month effective date for these requirements could result in covered financial institutions rushing to put something in place by the deadline while not having the opportunity to provide rigorous operational pressure-testing.

B. The section 314.6 exemption should be expanded.

Section 314.6 of the Proposed Amendments adds exceptions from several requirements for covered financial institutions "that maintain customer information regarding fewer than five thousand consumers." The purpose of the FTC adding this section is to "reduce burden on smaller financial institutions."[28] The exceptions would exempt qualifying financial institutions from the following:

- 314.4(b)(1) – requiring a written risk assessment.
- 314.4(d)(2) – requiring continuous monitoring or annual penetration testing and biannual vulnerability assessments.
- 314.4(h) – requiring a written incident response plan.
- 314.4(i) – requiring an annual written report by the CISO to the Board.

Many small financial institutions, including a number of ACA members, have objectively limited operations in terms of number of employees and revenues, but handle large volumes of consumer account data for each of their clients on whose behalf they are collecting debts. Even very small financial institutions with relatively few clients could quickly exceed the threshold in the Proposed Amendment.

If the Commission moves forward with amending the Safeguards Rule, to make the exception more meaningful for small businesses, ACA strongly urges the Commission to modify the Proposed Amendments to provide exceptions for "financial institutions that maintain customer

[28] 84 Fed. Reg. 13,170 (Apr. 4, 2019).

information concerning fewer than ten thousand consumers." To further avoid stifling innovative new companies and small businesses that have limited revenue, ACA also recommends that the Commission adopt a revenue-based dollar amount exemption. The revenue-based dollar exception should be an alternative to the personal information volume threshold, such that an organization would be exempt if it meets either threshold (and is not required to meet both in order to be exempt).

In addition, the CISO requirement should be added to the section 314.6 exemptions. As discussed above, forcing small and low-revenue businesses to designate a CISO, whether by hiring or promoting an employee, or by outsourcing, could create an unduly burdensome expense on small financial institutions.

The Commission should also consider, in lieu of expanding the scope of the exempted provisions, that small entities be allowed to operate in compliance with the current Safeguards Rule instead of any amended, new Safeguards Rule.

C. Certain language from the section 314.4(b)(1)(i)-(ii) risk assessment and criteria requirements should be removed.

The proposed requirement in section 314.3(a),(b) references a risk-based information security program, including a written risk assessment. Section 314(b)(i)-(ii) further sets forth that the risk assessment shall include criteria for evaluating, categorizing, and assessing certain parts of the information security program. These express requirements are unnecessary and should be removed. The current Safeguards Rule already requires a risk-based assessment that inherently requires the application of criteria to perform the assessment. Such criteria are generally understood and should remain flexible based on "the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of the customer information at issue."[29] As discussed above, the Commission can always issue guidance on such criteria if it has concerns that financial institutions are not satisfying its expectations in this regard.

D. The flexibility in the section 314.4(c)(4) encryption requirement should be maintained.

[29] 16 C.F.R. § 314.3(a),(b).

Section 314.4(c)(4) allows covered financial institutions to maintain compensating controls in lieu of encryption where the latter is infeasible. The concept in the Proposed Amendment of "compensating controls" is crucial because encryption across all databases and systems holding personal information is not always feasible for covered financial institutions. For the reasons discussed above, the CISO approval component of the encryption requirement should not apply; instead the one or more employees coordinating the information security program under the current Safeguards Rule should perform that function.

In addition, if the Commission adopts an encryption requirement, it should only do so for the most sensitive forms of customer information, which is consistent with taking into account "the sensitivity of the customer information at issue" as the current Safeguards Rule allows. The relevant proposed amendment, with the exception of the infeasibility exception, would impose the requirement on all customer data, in-transit or in storage. Encryption can be costly, especially for small financial institutions. That approach is unduly burdensome and fails to allow for sufficient risk-based approaches that do not rely on encryption, especially for non-sensitive customer data.

E. The flexible section 314.2(e) encryption definition should be maintained, but approaches other than encryption should be permitted as well.

While ACA disagrees with imposing an across-the-board encryption requirement for the reasons discussed above, proposed Section 314.2(e) defines "encryption" as "the transformation of data into a form that results in low probability of assigning meaning without the use of a protective process or key." ACA members and other financial institutions employ different forms of encryption based on their risk and the specific data in question, necessitating a flexible definition that does not incorporate specific technical requirements. ACA appreciates that the definition of the term "encryption" in the Proposed Amendments is sufficiently flexible to enable different approaches consistent with the scope of the covered financial institution and its risks.

However, the Commission should allow for other mechanisms that are reasonable, and not only where encryption is infeasible. For example, the Commission should allow a financial institution to use methods such as tokenization, drive-level encryption, robust access controls and

auditing/logging capabilities to protect even sensitive data in the systems where it is stored in lieu of actually encrypting the data. In sum, all safeguards that reasonably protect the information should be permitted, and the Commission should not view encryption as the sole panacea for protecting consumer information.

IV. ACA Supports a Safe Harbor.

ACA supports the concept of the Commission providing a safe harbor for companies that comply with a third-party data security standard as long as doing so is optional and the standard does not become the "*de facto*" test of reasonableness for financial institutions that choose not to assess or certify to a third-party standard. Certifying to a third-party standard can be expensive, especially for small financial institutions, and financial institutions can have robust and compliant information security programs even if not following a third-party standard.

V. Conclusion.

For the foregoing reasons, ACA International respectfully requests that the Commission forego promulgating the Proposed Amendments. Alternatively, if it proceeds with the Proposed Amendments, ACA International requests the FTC carefully consider the recommendations mentioned above.

Respectfully submitted,

/s/ Leah Dempsey
Leah Dempsey
Vice President and Senior Counsel, Federal Advocacy
ACA International
509 2nd St., NE
Washington, DC 20002