Before the
FEDERAL TRADE COMMISSION
Washington, DC 20530

In the Matter of	)	Project No. P145407
	)	
Standards for Safeguarding Customer Information	)	
	)	
Safeguards Rule, 16 CFR Part 314	)	

COMMENTS OF INTERNET ASSOCIATION

I. INTRODUCTION

Internet Association ("IA")[1] appreciates the opportunity to submit comments in response to the Federal Trade Commission's ("FTC" or "Commission") July 13, 2020 Public Workshop ("Safeguards Rule Workshop"), regarding the proposed amendments to the Gramm Leach Bliley Act's ("GBLA")[2] Standards for Safeguarding Customer Information ("Safeguards Rule"). IA and its members strongly support and value effective data security safeguard mechanisms. Our member companies are responsible stewards of the personal data that is entrusted to their care, and they support policies that protect the privacy of user information online. Additionally, many of our member companies are leading global commercial cloud providers working to develop low cost, secure, scalable, and resilient cloud services. They provide cutting-edge "defense in depth" protections to keep data safe from a wide array of threats. These companies are constantly leveraging their security expertise, insight, and orientation to update cloud security capabilities and stay ahead of tomorrow's next attack.

[1] IA is the only trade association that exclusively represents leading global internet companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. IA believes the internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, IA works to ensure policymakers and other stakeholders understand these benefits. https://internetassociation.org/.

[2] *See* Federal Trade Commission, Standards for Safeguarding Customer Information, 84 Fed. Reg. 23354 (Apr. 27, 2020), https://www.federalregister.gov/documents/2020/04/27/2020-08800/postponement-of-public-workshop-related-to-proposed-changes-to-the-safeguards-rule.

IA and its members strongly support data security principles that are flexible, risk-based, scalable, and technology neutral. As currently written, the Safeguards Rule provides a malleable framework that permits companies of all sizes to implement effective data security procedures. Overly rigid data security requirements will stifle innovation and reduce new market entrants' participation. We request that the Commission consider the following ideas discussed during its Safeguards Rule Workshop: (1) whether the current Safeguards Rule needs to be updated; (2) the impact of overly prescriptive amendments to the Rule; (3) the effects of additional obligations on selected service providers; and (4) the ramifications of an overly broad "financial institution" definition placing unreasonable burdens on non-financial institutions.

II. THE FTC's CURRENT SAFEGUARDS RULE EFFECTIVELY PROMOTES CUSTOMER INFORMATION SECURITY.

As other commenters noted on the record, the FTC's current Safeguards Rule provides the needed flexibility for companies to develop, implement, and maintain comprehensive data security programs.[3] In 2002, the FTC intentionally enacted the Safeguards Rule with general requirements and guidance giving companies the ability to customize their systems and respond to their individual needs without considering overly detailed and rigid requirements. Consequently, for more than 15 years, companies have been able to continually invest in robust customer data security systems to combat constantly evolving cyber threats. It is due to the FTC's well-reasoned regulatory approach that financial institutions have protected customer data while still maintaining a competitive business edge.

III. OVERLY PRESCRIPTIVE SAFEGUARDS RULE REQUIREMENTS WILL LIMIT INDUSTRY INNOVATION AND FINANCIAL INSTITUTION'S ABILITY TO ADAPT TO NEW CYBER THREATS.

The FTC's proposed Safeguards Rule places additional data security program requirements on financial institutions that will hinder their success. As discussed by the FTC Workshop's *Accountability, Risk Management, & Governance of Information Security Programs Panel*,[4] there

[3] *See e.g.*, Software & Information Industry Association, Project No 145407 (Aug. 2, 2019) ("[W]e believe the Safeguards Rule as currently promulgated is effective and that it must remain flexible if it is to enable compliance by small, innovative companies."); CTIA Comments, Project No. 145407 (Aug. 2, 2019) ("[T]he FTC proposes a sweeping overhaul of the data security standard for financial institutions within its jurisdiction, despite the fact that the Rule has effectively regulated data security…for close to 20 years.");Comments of Consumer Data Industry Association, Project No. 145407 (Aug. 2, 2019); Comments of the Electronic Transactions Association, Project No. 145407(Aug. 2, 2019); Comments of the National Automobile Dealers Association, Project No. 145407 (Aug. 2, 2019).

[4] Federal Trade Commission, Information Security & Financial Institutions: FTC Workshop to Examine Safeguards Rule, *Accountability, Risk Management, & Governance of Information Security Programs Panel* (July 13, 2020).

are multiple factors that financial institutions would need to reassess within their data security programs to ensure they are in compliance with the new Rule. For example, the panel considered how financial institutions would need to review their accountability mechanisms; oversight of the security program itself; costs associated with making changes to the security program; ability to provide third parties with access to the data security system, if such access is necessary to fulfill the new requirements; and the reporting requirements governing communications between the head of the security program and the Board of Directors.[5] Conversely, the current Safeguards Rule does not take such a prescriptive "one-size-fits-all" approach for data security program requirements. Instead the current Rule allows for companies to define the needed parameters of their information security programs and adapt, when necessary, to new threats to their system. Additionally, the current Safeguards Rule definitions are comprehensive enough and enacting the Commission's proposed changes would create a burdensome regime without any recognizable need to warrant such alteration. IA would recommend that the Commission maintain its current risk-based and flexible safeguards approach for financial institutions.

Further, the Commission's overly prescriptive requirements would limit the industry's ability to develop new and innovative approaches to data security. IA is concerned that the Commission's proposed changes will stifle growth of financial institutions, which could have detrimental downstream effects for some of our smaller members. The benefit of the current Safeguards Rule is that it allows financial institutions to scale their security programs to meet their needs while still being able to react to security threats when they arise. The current Rule provides financial institutions the flexibility to rapidly make real-time decisions to protect customer data without the concern of FTC enforcement action. Without this flexibility in the Safeguards Rule, many financial institutions may not be able to take the necessary steps to resolve new cybersecurity threats due to the onerous requirements the Commission has proposed. Therefore, we recommend the Commission adhere to its current Safeguards Rule and continue to allow the industry to grow and flourish.

IV. THE PROPOSED SAFEGUARDS RULE PLACES SIGNIFICANT ADDITIONAL COMPLIANCE BURDENS ON A FINANCIAL INSTITUTION'S SELECTED INFORMATION SERVICE PROVIDERS.

A. Where companies operate as a service provider for a financial institution, the proposed changes to the rule would require potentially significant additional requirements to their information service programs.

In accordance with the current Rule, "financial institutions must take reasonable steps to select and retain service providers capable of maintaining the required "safeguards"

[5] *Id.*

articulated by the Rule."[6] The current Rule only requires "this assessment of the service provider's safeguards at the onboarding stage." However, in the proposed amendments to the Safeguards Rule, "financial institutions would be required to monitor their service providers on an ongoing basis to ensure that they are maintaining adequate safeguards to protect customer information that they possess or access."[7] This not only creates an additional burden for financial institutions, but also places selected service providers under constant surveillance by their financial institution clients. Thus, service providers would be mandated to make substantial updates to their systems based on the newly proposed Rule to maintain their clients' business. Further, these changes would be very costly to the service provider, especially in light of the COVID-19 global public health emergency.

B. The FTC's proposed changes would also require additional future assessments of each company's information service program and adequacy of safeguards under the rule.

Specifically, the FTC proposes an addition to testing and monitoring under Section 314.4(d),[8] which would require "regular testing or monitoring to include either (1) continuous monitoring; or (2) annual penetration testing, in which assessors attempt to circumvent or defeat the security features of an information security plan, and biannual vulnerability assessments, which are designed to detect publicly known vulnerabilities."[9] However, the current Rule only requires "[r]egularly test[ing] or otherwise monitor[ing] the effectiveness of the safeguards' key controls, systems, and procedures, including . . . [tests that] detect actual and attempted attacks on, or intrusions into, information systems."[10] While IA acknowledges that the new proposal provides some flexibility, it fails to account for the fact that continuous monitoring or annual penetration testings are extremely burdensome on service providers, especially for service providers with multiple client accounts that demand the implementation of these protocols. Currently, service providers may plan for these assessments to ensure data security programs are running properly. However, if these newly proposed amendments are adopted, service providers could either (1) face constant monitoring from financial institutions, which would require additional resources and staff; or (2) be subjected to annual randomized penetrations for each financial institution client they serve. In IA's view both seem like unduly burdensome requirements that lack adequate justification.

V. THE PROPOSED AMENDMENT TO THE SAFEGUARDS RULE DEFINITION OF "FINANCIAL INSTITUTION" WOULD PLACE SIGNIFICANT BURDENS ON ENTITIES OUTSIDE OF FINANCIAL INSTITUTIONS.

[6] 16 C.F.R. § 314.4(f).
[7] Proposed 16 C.F.R. § 314.4(f).
[8] 16 C.F.R. § 314.4(d).
[9] Proposed 16 C.F.R. § 314.4(d)(2).
[10] 16 C.F.R. § 314.4(d).

The proposed Rule would amend the definition of "financial institution" to include finder companies "engaged in activities that are financial in nature or incidental to such financial activities." This would impose a significant burden on non-financial institutions, including small businesses that are conducting merely incidental activities. Many of IA's member companies work in the e-commerce industry and frequently serve as facilitators for small businesses to sell their items to a larger audience. Depending upon how these interactions are contractually constructed this change in the Safeguards Rule could have a significantly adverse impact on some of IA's smaller e-commerce members. Therefore, IA disagrees with the Commission's broader definition of a "financial institution" and encourages the Commission to continue forward with the current definition.

VI. CONCLUSION

IA appreciates the opportunity to provide the Commission feedback about its workshop and proposed amendments to the GLBA's Safeguards Rule. IA is a strong proponent of reliable and effective data security programs. However, the proposed amendments to the Safeguards Rule hinder the flexible, risk-based, and technology neutral approach that the FTC has been using for approximately the last two decades. IA believes that the current Safeguards Rule adequately regulates financial institutions and therefore such regulation should not be replaced with newer and more prescriptive requirements.