July 21, 2022

April Tabor
Acting Secretary of the Commission
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW, Ste. CC-5610
Washington, DC 20580

Re: Standards for Safeguarding Customer Information
16 CFR Part 314, Document No. 2021-25736

Dear Secretary Tabor,

On behalf of our members, ACA International,[1] the American Financial Services Association,[2] the Consumer Data Industry Association,[3] and the National Automobile Dealers Association[4] write to ask the Federal Trade Commission (FTC) to delay the effective date of the Standards for Safeguarding Customer Information rule (Final Rule) until December 2023.

Our members appreciate the FTC's work to protect customers' information, and they have every incentive to work alongside the Commission to ensure the right safeguards are in place to protect customers, their institutions, and the financial marketplace as a whole. At the same time, the residual effects of COVID-19 on the labor market and supply chain, as well as dueling regulatory demands and the technological changes required for proper compliance, make it difficult for covered entities to uplift their information security programs to meet the requirements in the Final Rule.[5] To that end, we are calling for a year-long delay of the effective date to give covered entities—and their service providers—more time to properly implement the Final Rule's modifications.

1. **Members cannot hire enough skilled people fast enough to feel comfortable that they have sufficient coverage.**

The current labor market shortage is still being felt by the financial services industry. The COVID-19 pandemic caused a major disruption in the American labor force, which has affected nearly every industry, including the financial activities industry. As of May 2022, there were 501,000 job openings in the financial activities sector that employers were actively looking to fill.[6] In May 2019, pre-pandemic levels of job openings were significantly lower, at 307,000.[7] This labor shortage has made it difficult for covered entities to find and hire the skilled workers they need to adjust their information security programs to be in line with the Final Rule. Moreover, the deficit in skilled workers is even greater when looking specifically at

[1] https://www.acainternational.org/
[2] https://afsaonline.org/
[3] https://www.cdiaonline.org/
[4] https://www.nada.org/
[5] 86 FR 70272, December 9, 2021.
[6] U.S. Bureau of Labor Statistics, *Job openings, hires, and total separations by industry, seasonally adjusted*, available at https://www.bls.gov/news.release/jolts.a.htm (July 6, 2022).
[7] U.S. Bureau of Labor Statistics, *Job Openings and Labor Turnover – May 2019*, available at https://www.bls.gov/news.release/archives/jolts_07092019.pdf (July 9, 2019).

cybersecurity professionals. One study suggests that the shortage of cybersecurity professionals in the United States has doubled (from 300,000 to 600,000) in recent years.[8] With every organization (not just financial institutions) vying for the same scarce talent, it is extremely difficult to fill open requisitions for positions that are crucial to an effective information security program. As you know, the Final Rule demands that covered entities "utiliz[e]. . . qualified information security personnel . . . *sufficient* to manage your information security risks and to perform or oversee the information security program."[9]

2. **The Final Rule is not the only major initiative on the docket.**

Much has been made of the growing patchwork of privacy and data security laws, rules, and guidance in the United States and the burdens it places on covered entities.[10] This is an active space, with no signs of slowing down. For example, concurrent with their preparations for the Final Rule, our members are preparing for the entry into force of various amendments to the California Consumer Privacy Act (CCPA) on January 1, 2023. While these CCPA amendments share a focus on consumers' personal information, they are quite different from the Final Rule. Indeed, the CCPA amendments will require retooling and reimagining of information systems that goes well beyond systems that support individual customer relationships, including those that touch personal information about employees and business-to-business contacts. While our members are not strangers to competing regulatory demands, the unavoidable linkage to information technology increasingly strains resources (both people and budgetary) that are already spread paper thin.

3. **Equipment and external resources are in short supply.**

Additionally, some of the Final Rule's modifications require technological changes to the existing security program. These changes include the establishment of a multi-factor authentication system,[11] a move toward least privileged access, and an encryption process for all forms of customer information. While the amount of work required to fulfill these directives will depend on the entity's current program, in almost all cases these technological changes will require significant investments of time and money to implement. By way of example, adopting a least privileged access model across all customer information applications and datasets is very complex.

Even for organizations that are far along in identifying and harmonizing the various roles that exist in their corporate structure, assigning the proper permissions requires an in-depth look at the business functions these roles are expected perform, along with fine-tuning around exceptions that may surface within those roles.[12,13] It will be a challenge to reconfigure systems and/or procure additional encryption tools, and thoroughly testing the new systems will add additional time to implementation. Furthermore, due to recent supply chain issues, it has been difficult for entities to secure the equipment they need to upgrade their IT.

---

[8] Cyber Seek, *Cybersecurity Supply/Demand*, available at https://www.cyberseek.org/heatmap.html.
[9] 86 FR 70272, Sec. 314.4(e)(2).
[10] Castro et al., *The Looming Cost of a Patchwork of State Privacy Laws*, available at https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/ (January 24, 2022).
[11] 86 FR 70272, Sec. 314.2.
[12] This is process is even more complex when you consider that the Final Rule requires covered financial institutions to adopt these practices not only for internal (*i.e.*, employee and agent) access to customer information, but also for customers' own access to their information.
[13] 201 C.M.R. 17.04(3), (5) available at https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download (requiring encryption of "personal information" in transit and when stored on portable devices to the extent technically feasible).

A decrease in the production of semiconductor computer chips coupled with an increase in demand for laptops and personal computers during the pandemic has led to a shortage of available computers. A U.S. Department of Commerce report stated that "there is a significant, persistent mismatch in supply and demand for chips," [14] decreasing inventory to less than five days in 2021. This lack of inventory has decreased the amount of time that covered entities have to properly develop the software needed for the technological changes.

4. **Preparing a written risk assessment that conforms to the FTC's specific criteria—the bedrock of the Final Rule—is a manual, subjective, time-consuming process.**

As you know, one of the five primary ways in which the Final Rule modifies the FTC's current rule is through the establishment of specific criteria for each covered financial institution's written risk assessment. As a result, many (if not most) covered entities will need to modify not only their methods for evaluating the risks they face, but also the manner in which they document these risks—even before they do any work to mitigate these risks and bring their information security program more in line with the FTC's updated requirements. This is not straightforward and requires ongoing care and feeding by qualified cybersecurity professionals which are in short supply, as noted above.

Furthermore, not only do covered entities need to meet the requirements of the Final Rule themselves, they must also ensure that their service providers meet many of these same complicated requirements, and that contracts are amended to reflect these changes. This process is particularly cumbersome and time consuming. In many cases it is outside of the control of the covered entities themselves. As a result, the difficulties many covered entities have in meeting internal compliance are only multiplied by the myriad differing service provider capabilities, technologies, receptiveness, and internal challenges of their own. Covered entities simply need more time to ensure their service providers are taking the steps required under the Final Rule.

The covered entities affected by the modifications in the final rule are committed to safeguarding their consumers' information. In order to properly implement the new requirements, we are requesting that the FTC delay the applicability date until December 9, 2023, in order to allow time for proper staffing, technological systems' changes including thorough testing, service provider compliance, and an increase in inventory to be able to best serve our consumers.

We appreciate the FTC considering this request. Please contact Leah Dempsey (ldempsey@bhfs.com), Celia Winslow (cwinslow@afsamail.org), Eric Ellman (eellman@cdiaonline.org) or Paul Metrey (pmetrey@nada.org) with any questions.

Sincerely,

ACA International
American Financial Services Association
Consumer Data Industry Association
National Automobile Dealers Association

[14] U.S. Department of Commerce, *Results from Semiconductor Supply Chain Request for Information*, available at https://www.commerce.gov/news/blog/2022/01/results-semiconductor-supply-chain-request-information (January 25, 2022).