Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

CDIAONLINE.ORG

August 18, 2022

Via Electronic Delivery to
cyberamendment@dfs.ny.gov

New York State Department of
Financial Services
1 State Street
New York, NY 10004-1511

RE: Pre-Proposed Second Amendment Cyber Security Requirements for Financial Services Companies (23 NYCRR 500)

To Whom It May Concern:

The Consumer Data Industry Association (CDIA) submits this comment letter in response to the New York State Department of Financial Services (DFS)'s invitation for comments on its pre-proposal to amend its Cybersecurity Regulation (23 NYCRR 500). In short, the pre-proposed amendments raise more than a few initial questions and concerns, not least of which is the propriety of imposing potentially new cybersecurity requirements on businesses at a time when many are actively assessing and revising their cybersecurity programs for compliance with new Federal Trade Commission (FTC) Safeguards Rule requirements, which may or may not overlap with DFS's pre-proposals. Should DFS decide to move forward, we urge the agency to afford sufficient process and time for formal comment and review as well as implementation should any amendments ultimately become effective.

CDIA is the voice of the consumer reporting industry, representing consumer reporting agencies (CRAs), including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

On July 29, 2022, DFS released pre-proposed amendments to its Cybersecurity Regulation, a state regulation requiring covered entities to, among other things, regularly assess their cybersecurity risks and develop and implement programs to effectively address those risks. CDIA members that fall under the New York Consumer Credit Reporting Agency Registration provisions (23 NYCRR Part 201) may be covered entities under the Cybersecurity Regulation.

DFS's pre-proposed amendments to the Cybersecurity Regulation are extensive and highly prescriptive. The amendments would mandate a 24-hour notification for cyber ransom payments, annual independent cybersecurity audits for larger covered entities, increased requirements for directors' expertise and knowledge of cyber risk, and onerous new restrictions on privileged access. The amendments would also create a distinct category of covered entities, called "Class A companies," defined as covered entities with 2,000 employees or more than $1 billion in gross annual revenues averaged over the last three years from all businesses, who would be subject to several additional new audit and secure control requirements, including, but not limited to, annual audits of cybersecurity programs, risk assessments conducted every three years by external experts, and strict password controls.

Although CDIA and its members appreciate the opportunity to review and comment on the pre-proposed amendments at this stage, the short window that DFS opened for comment is insufficient for CDIA's members to fully bench test and consider the programmatic implications of the amendments in order to provide meaningful commentary on all of the proposed changes. Further, because this early release does not have the benefit of agency commentary or similar statement of purpose, the rationale and basis for certain proposed amendments is unclear.

Initial reactions from some members, however, suggest concerns over several pre-proposed amendments, including textual clarity, such as whether pre-proposed subdivision 500.8(b) requires review and update of cybersecurity program materials "as necessary" or "at least annually"; and whether the pre-proposed definition "covered entity" that would be amended to include "entities that are also regulated by other government agencies" could potentially touch all businesses operating in New York. Some members also raised concerns about the pre-proposed definition for the term "independent audit"; changes to the certification requirement; references to specific required controls, such as "vaulting," which are not the only possible applicable controls and may become outdated in the future; and whether the effective date in the pre-proposal would provide sufficient time for covered entities to come into compliance. Moreover, many entities covered by DFS's Cybersecurity Regulation are also subject to the FTC's Safeguards Rule, which was recently revised to expand its coverage and require covered entities to comply with new information security requirements, and some companies are still in the process of reviewing and updating, where necessary, their cybersecurity programs to ensure Safeguards Rule compliance. Changes to the Cybersecurity Regulation would force many of these companies back to the drawing board in order to assess compliance and any overlap with any changes to state and federal regulations.

Given the breadth and scope of the pre-proposed amendments, should DFS formally propose these rule amendments, CDIA strongly encourages DFS to afford sufficient time for CDIA members and other stakeholders to review and consider the amendments and to provide thoughtful and data-driven comments. CDIA also strongly encourages DFS to provide greater transparency about its thought process and regulatory approach, including the impetus for and rationale underlying any rule amendments. For instance, it would be useful to stakeholders to

know the reasoning behind the definitional thresholds for "Class A" covered entities and have an opportunity to comment on whether that threshold is appropriate. In addition, it would be very helpful for the agency to share its reasoning and conclusions on the rulemaking decisions in general, including any expert opinions, pre-proposal facts gathered, and economic or business impact analyses, and to identify the purpose of each amendment or what issue(s) each is designed to solve.

We appreciate the opportunity to comment on DFS's pre-proposed amendments to its Cybersecurity Regulation and hope the agency will find these comments useful.

Sincerely,

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs