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

January 9, 2023

Via Electronic Delivery to
cyberamendment@dfs.ny.gov

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

RE: Proposed Second Amendment to 23 NYCRR 500

To Whom It May Concern:

The Consumer Data Industry Association (CDIA) submits this comment letter in response to the invitation of the New York State Department of Financial Services (DFS) for comments on its proposed amendment to its Cybersecurity Regulation (23 NYCRR 500). 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.

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.

Following a comment period for a "pre-proposed" version, on November 9, 2022, DFS published 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 appreciates DFS's consideration of stakeholder comments and concerns voiced in response to the earlier "pre-proposed" version of this amendment. While important changes have been made from the earlier proposals, in particular the relaxing of implementation periods for some technical requirements, the proposed amendments still raise significant questions and concerns. Broadly, CDIA remains concerned with the proposal's breadth and highly prescriptive nature, particularly in light of recently revised federal requirements under the Safeguards Rule.[1] We address our specific concerns below.

[1] 16 C.F.R. Part 314.

1. DFS should reconsider imposing additional cybersecurity requirements on financial institutions that have recently been in the process of rebuilding their information security programs.

CDIA questions the propriety of imposing additional cybersecurity requirements on businesses at a time when many are actively assessing and revising their cybersecurity programs for compliance with new federal regulations. Financial institutions covered by DFS's Cybersecurity Regulation are also subject to the Federal Trade Commission's Safeguards Rule, which was recently revised to expand its coverage and require covered entities to comply with new information security requirements. Those entities have either been or may still be in the process of reviewing, updating, and even rebuilding, where necessary, their information security program to ensure Safeguards Rule compliance. This is to say nothing of other potential rule changes from other federal regulators that would further impact many businesses' cybersecurity programs.[2] Introducing regulations that are more prescriptive than or potentially bump up against federal rules to businesses right now would impose considerable cost and burden, forcing many of them back to the drawing board in order to assess compliance and any overlap with any changes to state and federal regulations. It also takes institutions' focus off of identifying new and changing emergent risks to focus on technical compliance issues.

2. DFS should address specific areas of textual vagueness.

CDIA is concerned with the proposal's breadth and highly prescriptive nature as well as its textual clarity. In particular, certain terms and standards expressed in the proposed amendment, including "timely" (proposed subdivision 500.4(c)) and "sufficient expertise and knowledge" (500.4(d)(3)), could afford to be further defined, as they are vague and thus create legal uncertainty. Additionally, proposed subdivision 500.8(b) is ambiguous as to whether covered entities must review and update their cybersecurity program materials "as necessary" or "at least annually."

In addition, CDIA recommends replacing the term "test" in subpart (d) of Section 500.16 with "exercise," so the subpart would require that each covered entity periodically, but at least annually, "exercise" its incident response plans, business continuity and disaster recovery plan, and ability to back up its systems. While testing and exercising are closely related and sometimes used interchangeably, they are distinct in information technology (IT) parlance and

[2] *See* Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 Fed. Reg. 55833 (Sept. 12, 2022) (seeking public comment on how to structure implementing regulations for reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act), https://www.govinfo.gov/content/pkg/FR-2022-09-12/pdf/2022-19551.pdf; Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies, 87 Fed. Reg. 13524 (Mar. 9, 2022), https://www.govinfo.gov/content/pkg/FR2022-03-09/pdf/2022-03145.pdf.

offer different ways of identifying deficiencies in cybersecurity plans and procedures. Periodically conducting exercises—simulating emergencies designed to validate the viability of the organization's IT or security plan and allowing staff to execute their roles and responsibilities as they would in an actual emergency—would seem more likely to serve the objective of ensuring critical personnel are adequately trained and prepared to respond to cybersecurity events.

3. The regulation should permit independent audits by employed internal audit teams.

The proposed definition of the term "independent audit" for purposes of audit requirements only includes external auditors. This requirement thus rejects established *internal* audit practices, whereby larger companies including CDIA members are able to use employed auditors to objectively assess operations and report directly to the board of directors instead of having to pay third party firms for the same work.

* * *

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

Sincerely,

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