ELECTRONIC TRANSACTIONS ASSOCIATION
1620 L Street NW, Suite 1020
Washington, DC 20036
202.828.2635
electran.org

August 14th, 2023

Superintendent Adrienne Harris
New York State Department of Financial Services
1 Commerce Plaza
Albany, NY 12257

Via Electronic Mail to: cyberamendment@dfs.ny.gov

Re: Comments on Revised Proposed Second Amendment to Cybersecurity Regulations (23 NYCRR 500)

Superintendent Harris,

On behalf of the Electronic Transactions Association ("ETA"), the leading trade association for the payments industry, we appreciate the opportunity to provide the comments below on the Department of Financial Services' ("DFS") revised proposed second amendment to cybersecurity regulations.

COMMENTS

1) Section 500.4(d)(1) states that a covered entity's senior governing body shall "exercise effective oversight of the covered entity's cybersecurity risk management." A covered entity should be allowed to designate a cybersecurity committee created and with proper oversight by the senior governing body to provide oversight in compliance with this regulation. The definition of "senior governing body" in the proposed amendments means "the board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer or officers of the covered entity responsible for the covered entity's cybersecurity program." Therefore, the board of a covered entity would be able to create a cybersecurity committee that would be responsible for the senior governing body requirements under the proposed amendments. However, the amendment language should be expanded to clarify that covered entities can allow executive management to be responsible for the cybersecurity program requirements of the senior governing body. The current language in the proposed amendments would only allow executive management to have such oversight if the entity does not have a board of directors or cybersecurity committee. As cybersecurity issues rapidly change and evolve, covered entities should be given flexibility to set up the correct cybersecurity oversight structure for their organization. **Section 500.4(d)(1)**

2) Given the varying size and complexity of different technology stack and operating models across the industry, the amendment should be clarified that covered entities should take a risk-based approach to the implementation of the testing program. **Section 500.5(a)(1)**

3) The proposed amendments would require a covered entity to report a cybersecurity event to the DFS as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred. The DFS should make it clear that a covered entity's determination that a cybersecurity event has occurred would allow for the covered entity to

thoroughly investigate and verify the specifics of such event before the 72-hour time-period commences. This would prevent covered entities from hastily reporting what could be incomplete or incorrect information quickly gathered to meet the 72-hour incident reporting requirement. Moreover, the scope of the amendment should be narrowed to focus on cybersecurity events that impact products and services provided to residents of New York state and such requirements would not be applicable to products and services that are not offered to residents of New York. **Section 500.17**

4) The proposed amendments have moved the requirement that entities notify DFS regarding security events that occur at a third-party service provider to Section 500.17(a)(1). This change creates an alignment issue, specifically with respect to the events described in Section 500.17(a)(i) and (iii). A direct reading of Section 500.17(a)(1)(i) now suggests that a cybersecurity event occurring at a third-party service provider could simultaneously be a notifiable event impacting the covered entity—this lacks logical coherence. Similarly, a direct reading of Section 500.17(a)(1)(iii) suggests that the cybersecurity event occurring at a third-party service provider where an unauthorized user gains access to a privileged account would be a reportable event, regardless of whether the event impacted the covered entity. This section requires modification to ensure clarity and reporting obligations should be tied to the reasonable likelihood of material impact to a covered entity. **Section 500.17(a)**

We appreciate you taking the time to consider these important issues. If you have any questions or wish to discuss any aspect of our comments, please contact me or ETA Senior Vice President of Government Affairs Scott Talbott at Stalbott@electran.org.

Respectfully Submitted,

Brian Yates
Senior Director, State Government Affairs
Electronic Transactions Association
202.677.7714 | byates@electran.org