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

January 9, 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 Proposed Amendments to Cybersecurity Rules (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") proposed amendments to cybersecurity regulations.

COMMENTS

1) The required audit should be able to be performed by the company's internal audit function, as long as the internal audit function is truly independent of the business being audited. To effectuate this change, the definition of "independent audit" should be revised to include "an audit conducted by the covered entity's internal audit function, provided that (1) the internal audit function do not report to the business being audited (e.g., reporting instead through the Finance function), (2) the internal audit personnel do not have their compensation determined by personnel that report to the business being audited, and (3) the internal audit function is free to make decisions not influenced by the business being audited." **Section 500.1(f)**

2) ETA suggests that the Superintendent consider defining the scope of the annual independent audit proposed in Section 500.2(c). An annual, in-depth audit of all aspects of the cybersecurity program of a larger covered entity with many complex information systems could be so complex and time-consuming as to be effectively impracticable. Given the complexity and breadth of information systems within large, covered entities, the scope of the required annual audit must be clarified to cover a depth and breadth that is, in practical terms, possible for covered entities to complete annually. ETA suggests that the Superintendent consider whether an annual independent audit of key performance indicators for the cybersecurity program, potentially in combination with regular in-depth audits of individual components of the cybersecurity program, might address the risks this provision aims to mitigate. Further, to avoid burdensome simultaneous audits, the audits should be focused only on certain key performance indicators or a single element on a rotating basis. Covered entities will benefit from further clarity as to the scope of the annual audit and a provision allowing for in-depth audits of individual components of complex cybersecurity programs to supplement a higher-level annual audit. **Section 500.2 (c)**

    a) The annual audit requirement should be changed to a biennial or every two-year requirement. An annual independent auditing requirement will excessively burden covered entities with more costs and additional distractions away from operating core business functions. Moreover, covered entities may struggle to locate an "independent auditor" as the new rule will cause a backlog of audit requests that will challenge annual compliance deadlines.

b) Companies with a global presence conduct thorough audits at the parent level, complying with international standards in addition to states including New York. The DFS should allow companies who comply with international standards such as ISO to be exempt from an additional subsidiary audit and remain able to conduct audits on a parent level.

3) The definition of *penetration testing* applies to "testing the security of information systems by attempting to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from **outside** or inside the covered entity's information systems." Further clarification is needed of how the term "outside" is applied in this definition. Specification is needed to determine what type of circumvention is considered to be "outside" of the information system. **Section 500.1(h)**

4) Section 500.5(d) would require covered entities to "document material issues found during testing and report them to its senior governing body and senior management." The amendment does not define "senior management" and it is unclear what distinctions might exist between "senior management" and the defined terms *senior governing body* and *senior officer(s)*. Moreover, the bulk of the amendment contemplates mandatory reporting only to the "senior governing body." *See* Section 500.3 (written policies shall be approved at least annually by the senior governing body); Section 500.4(c) (the CISO shall timely report to the senior governing body regarding material cybersecurity issues); and Section 500.16(2)(iii) (covered entities' business continuity and disaster recovery plan must include a plan to communicate with essential persons, including the senior governing body). **Section 500.5**

a) If material issues found during testing must be reported to a separate "senior management" entity, ETA suggests that the Superintendent define that term and explain any distinctions between the "senior management" and the "senior governing body" which is to receive the majority of reports contemplated in the amendment.

5) The amendment makes multiple references to "vulnerabilities," and it is unclear whether the Superintendent intends those references to only cover software code vulnerabilities as that term is understood in the software development industry or a different, broader definition of "vulnerabilities" which could be used to describe various points of potential risk exposure throughout information systems and network architecture. **Sections 500.1, 500.3, 500.5**

a) Specifically, the proposed definition of *risk assessment* incorporates "threat and vulnerability analyses" (500.1(n)); 500.3(o) requires written policies and procedures to include "vulnerability management"; and 500.5 also requires "written policies and procedures for vulnerability management" which must include "automated scans" and "manual review" for "discovering, analyzing and reporting vulnerabilities," a monitoring process for notification of "new security vulnerabilities," and risk-based remediation of vulnerabilities. Covered entities would benefit from clarification as to whether the "vulnerability analyses" that must be part of annual risk assessments encompasses a different scope than the "vulnerability management" policies and procedures of 500.3 and 500.5.

b) Section 500.5(a) of the proposed amendments add requirements for periodic vulnerability scans and penetration tests, including automated scans or manual system reviews at a frequency determined by the risk assessment and promptly after major system changes. The amendments should be revised to allow a risk-based decision regarding which environments and systems to scan and test, taking into account the criticality of systems and the sensitivity of data held by those systems.

c) Sections 500.5(b)-(d) of the proposed amendments also require a monitoring process to ensure covered entities are promptly informed of new security vulnerabilities, timely remediate vulnerabilities based on risk, document material issues found during testing, and report those issues to the covered entity's senior governing body. Given the lack of a definition of "material" issues, it should be clarified that the timely remediation and reporting of identified vulnerabilities should apply only to critical- and high-risk vulnerabilities.

6) ETA seeks clarity with respect to the qualifier "[a]s part of its cybersecurity program" that begins Section 500.13 of the amendment. Traditionally, asset management functions such as maintaining an asset inventory are the responsibility of the Information Technology department within an organization, rather than the cybersecurity department. As such, it is likely that the IT department within most covered entities is currently responsible for maintaining policies and procedures with respect to asset inventory and the associated responsibilities therewith. ETA suggests that the Superintendent clarify whether compliance with the amendment would require covered entities to move their asset management functions within their cybersecurity organizations, to manage the policies and procedures that are to be followed by the separate IT department, or whether a governance structure in which cybersecurity would have some oversight with respect to IT departments' asset management policies would suffice. Importantly, given the diversity of corporate structures, ETA is not seeking a mandate of a specific corporate organizational structure, but rather clarity of what would be sufficient to satisfy the requirements of this section. **Section 500.13**

a) The Superintendent should consider providing clarity as to what assets must be covered in the asset inventory, utilizing a risk-based approach to achieve an appropriate cost-benefit outcome, particularly given the speed and volume at which assets are developed and modified for many covered entities.

7) Section 500.16 will cause practical challenges for covered entities to comply with annually testing incident response plans with all critical staff, including senior officers and the CEO. The implementation and testing of incident response plans every year will present difficulties for covered entities to coordinate critical staff and the senior officers to devote considerable time away from focusing on the core business function of the entity. Testing incident response plans should be changed to a biennial or every two-year requirement to allow for more reliable compliance by senior officers over a 2-year period to ensure their full engagement in the incident response plan process. **Section 500.16**

a) Under Section 500.16(d)(1), the amendments would require a covered entity's highest-ranking executive to be involved in the testing of the company's incident response plan through tabletop exercises. Most tabletop exercises involve C-suite employees on an as-needed and appropriate basis, addressing escalations and issues with relevant stakeholders. We agree that it is important for senior leaders to manage cybersecurity programs. However, it is unnecessary and may create

inefficiencies to mandate a covered entity's highest-ranking executive to be extensively involved in all aspects of the annual testing of the entity's incident response plan.

b) Section 500.16(b)(v) of the amendment would require covered entities to include, in their incident response plans, "identification of requirements for the remediation of any identified weaknesses in information systems and associated controls." ETA suggests that the Superintendent consider defining the types of "weaknesses" that would require remediation under the amendment. Every information system has some degree of "weaknesses" that are impracticable to remedy. This section should be revised to require covered entities' incident response plans to include identification of weaknesses which were exploited or otherwise had a causal nexus with the cybersecurity incident, and an identification of requirements for the remediation of those specific identified weaknesses, rather than any potentially "identified weakness" in information systems.

8) The proposed amendments require covered entities to report cybersecurity incidents within 72 hours to DFS and notify any extortion payments in response to an extortion demand within 24 hours. Clarification is needed of when the 72-hour reporting period begins, at the time of a third-party notification or otherwise. Moreover, this brief time span should be lengthened to allow regulated entities enough time to thoroughly investigate and process the ransomware threat before reporting what could be incomplete or incorrect information quickly gathered to meet the 72 hour or 24-hour reporting requirements. **Section 500.17**

a) The proposed amendments expand when a covered entity should report a cybersecurity event to include (1) "where an unauthorized user has gained access to a privileged account" and (2) where ransomware had been deployed "within a material part of the covered entity's information system." The first requirement should be revised to a narrower definition of unauthorized access to a "privileged account" (it should only include accounts that provide access to critical IT systems or that access nonpublic information). Absent a narrower definition of "privileged account" that considers whether access to the account would materially impact nonpublic information, the first requirement may result in increased reporting and thus burdens on covered entities with limited consumer benefits. For instance, covered entities may be required to report events where privileged account access is of little value (e.g., no indication of access to nonpublic information or key systems). **Section 500.17(a)(1)(iii)**

9) Section 500.17(a)(2) would require that "**Within 90 days of the notice of the cybersecurity event**, each covered entity shall provide the Superintendent electronically in the form set forth on the department's website **any information requested** regarding the investigation of the cybersecurity event" (emphasis added). As written, this requirement could be impossible to meet. Should the Superintendent request information from a covered entity 88 days after the covered entity submitted notice of a cybersecurity event, the covered entity would have only two days to attempt to gather the additional information requested. ETA suggests that this provision be amended to require a response to any information requested within 90 days of the request for additional information. **Section 500.17**

a) Additionally, the proposed amendments state that covered entities will have a "continuing obligation to update and supplement the information provided," without clarifying the scope of this obligation. The Superintendent should clarify that such supplemental reports are only

required when substantially new or different information becomes available with the "continuing obligation" ending once the incident at issue has been mitigated and resolved.

10) Section 500.17(a)(3) would require each "covered entity that is affected by a cybersecurity event at a third-party service provider [to] notify the Superintendent. . . of such cybersecurity event." Given the broad range of possible interpretations for the phrase "affected by," ETA suggests that the Superintendent amend this provision to require notification of third-party service provider cybersecurity incidents that meet the same thresholds for reporting as those applicable directly to covered entities – namely, the conditions laid out in Section 500.17(a)(1). Additionally, it should be made clear that the reporting obligation for third party incidents arises when the thresholds of Section 500.17(a)(1) are met with respect to the covered entity. A cybersecurity incident could have a reasonable likelihood of substantially harming the normal operations of the third-party service provider but have a very low likelihood of any impact to the covered entity. Thus, only those third-party cybersecurity incidents that create one or more of the conditions of Section 500.17(a)(1) for the covered entity should give rise to a reporting obligation for that entity. **Section 500.17**

11) Notices of Compliance with Section 500 are a substantial undertaking, requiring a great deal of information gathering and scrutiny. The proposed Section 500.17(b)(2) would require both the CISO and the covered entity's highest-ranking executive (such as the CEO) to sign the certification of compliance. Such certification should not be required from both the CISO and highest-ranking executive. Rather, each covered entity should be able to determine whether the CISO or the highest-ranking executive, or any other appropriate personnel (such as a senior officer responsible for cybersecurity), is best positioned to evaluate the entity's cybersecurity program. Additionally, many high-ranking executives would require more than thirty days to be able to review all the material necessary to confirm compliance with the requirements of Section 500. Therefore, ETA suggests that Section 500.17 go into effect 180 days, rather than 30 days, after the effective date of the amendment, to give high-ranking executives sufficient time to review all information relating to covered entities' cybersecurity programs. **Section 500.17**

12) Under the proposed amendments, covered entities would be required to notify the Superintendent within 24 hours of making a ransom payment under Section 500.17(c)(1), as well as provide a written description within 30 days of why the payment was necessary, alternatives considered, and sanctions diligence conducted under Section 500.17(c)(2). The Superintendent should consider explicitly addressing the confidentiality of documentation and information submitted in connection with a request (e.g., under Section 500.17(a)(2)) and in connection with reporting requirements such as ransom payment reporting. **Section 500.17**

    a) The data required under the regulations is of a highly sensitive nature and proprietary, and we urge DFS to provide assurances with respect to its own data security practices. Such data (including detailed reports of non-compliance gaps under Section 500.17(b)) could make the DFS vulnerable to cyberattacks, and if subject to unauthorized access, could be used by malicious actors to materially impact a covered entity. Accordingly, it would be helpful for DFS to confirm the security standards to which it adheres, and ensure they are appropriate given the volume and sensitivity of the data entrusted to DFS.

13) Section 500.20 under the proposed amendments defines a violation as the commission of a single prohibited act (such as the failure to secure or prevent unauthorized access to an individual's or entity's nonpublic information) or any 24-hour period of noncompliance with any section of Part 500. A violation constituting "the failure to comply for any 24-hour period with any section or subsection of this Part" does not allow covered entities (that are acting in good faith) sufficient time to remedy even minor compliance gaps. Moreover, for nearly all significant cybersecurity events, 24 hours is not enough to remedy an exploited compliance gap that resulted in unauthorized access or a failure of security. **Section 500.20**

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