COMMITTEE ON INSURANCE LAW

FREDERIC M. GARSSON
CHAIR
fred.garsson@saul.com

SAPNA MALOOR
SECRETARY
sapna.maloor@chubb.com

January 9, 2023

Via Email to joanne.berman@dfs.ny.gov
Ms. Joanne Berman
New York Department of Financial Services
One State Street Plaza
1 State Street
New York, NY 10004

Re: **Proposed Second Amendment to 23 NYCRR 500 on Cybersecurity Requirements for Financial Services Companies**

Rulemaking I.D. No. DFS-45-22-00025-P

Dear Ms. Berman:

The Committee on Insurance Law of the New York City Bar Association is grateful for the opportunity to offer comments on the proposed Second Amendment to 23 NYCRR Part 500, Cybersecurity Requirements for Financial Services Companies.[1]

The Committee comprises lawyers representing a diverse cross-section of the insurance community, including lawyers in private practice, in-house counsel at insurance carriers and producers across multiple lines of insurance business, trade association officials, regulators, policyholder lawyers, insurance arbitrators and other types of insurance professionals. This letter represents the views of the Committee as a whole and not necessarily those of any particular member thereof.

The Committee's comments on the proposed amendment are as follows:

- **Forms not included in the regulation.** In several places the proposed amendments mandate reporting on forms to be developed by the Department of Financial Services ("DFS") and published on its website. See, *e.g.*, Secs. 500.17(a), (b) and (c) and 500.19(f). This raises a concern that DFS could develop forms that include requirements not specified in the regulation, which would violate the requirement under the State Administrative Procedure Act ("SAPA") that rules be promulgated through SAPA procedures and exempts

[1] NYS Register, November 9, 2022, Vol. XLIV Issue 45 at p. 26.

forms and instructions only if they do not have legal effect.[2] This is also a departure from the regulation's approach pre-amendment. Specifically, Appendix A (form of certification of compliance) and Appendix B (form of notice of exemption) would both be deleted by the amendment.

- **Rules that mandate outcomes, not processes.** The precise language of some new requirements can be interpreted to mandate outcomes, rather than requiring covered entities to take actions that are reasonably designed to achieve the outcomes. This is at odds with the spirit and overarching approach of the original regulation, and may be unrealistic given the nature of cyber threats. The provisions that cause concern are Sec. 500.14(a)(2) (protecting against malicious code) and Sec. 500.14(b) (monitoring anomalous activity).

- **Penalty escalation.** The proposed changes to Sec. 500.20 make any noncompliance within a 24 hour period an independent violation. No materiality threshold is applied. The proposal allows for mitigating factors to be considered in the calculation of a penalty, but the violation remains nonetheless. A concern is that a technical violation which occurs over an extended period despite a covered entity's reasonable compliance efforts could result in multiple violations, leaving the covered entity at the discretion of DFS to impose only a reduced penalty.

- **Elimination of the agent exemption from third party policy requirement.** Sec. 500.11(c) would be removed under the amendments. This provision granted to an agent, employee, representative or designee of a covered entity, that is itself a covered entity, an exemption from the requirement to develop a third party information security policy, as long as the agent, employee, representative or designee follows the principal's policy. This could have the effect of imposing on smaller entities burdensome administrative requirements that do not offer a correlative benefit in cybersecurity, insofar as these entities are following established policies of their principals.

  Apparently this provision was removed because it was perceived to be duplicative of Sec. 500.19(b). However, this latter provision is somewhat unclear as to scope. Specifically there is some ambiguity about whether agents are exempt altogether ("exempt from this Part") or only to the extent covered by the principal's systems ("and need not develop its own cybersecurity program to the extent . . . covered by the cybersecurity program of the Covered Entity.") Keeping Sec. 500.11(c) in effect on third party security systems would retain clarity for agents on this key aspect of compliance.

- **"Industry standard" encryption.** Under the amendments, Sec. 500.15 would be revised to require a written policy requiring encryption that meets industry standards. Sec. 500.7(b) would require a password policy that meets industry standards. In the fast-evolving world of cybersecurity, this could prove to be a vague standard for these aspects of data protection. This would result in DFS's having very broad discretion to determine whether the encryption or password policy implemented by a covered entity is sufficient. It would be preferable if the regulation merely required covered entities to implement an encryption standard and password policy, as the case may be, reasonably designed to shield sensitive information from unauthorized persons. This would represent a fairer standard that would still give DFS broad discretion to enforce encryption and password policies.

[2] SAPA § 2(b)(iv).

The Committee would be delighted to answer any questions or respond to any concerns that DFS may have regarding the foregoing matters. Feel free to respond to us by contacting the undersigned.

Very truly yours,

Frederic M. Garsson, Chair