Scott A. Sinder
202 429 6289
ssinder@steptoe.com

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.steptoe.com

Steptoe

November 11, 2022

M E M O R A N D U M

TO: **The Council**

FROM: **Scott Sinder**
Ashelen Vicuña
Sophia Breggia

RE: **Proposed Second Amendment to 23 NYCRR 500:**
"Cybersecurity Requirements for Financial Services Companies"

On November 9, 2022, New York's Department of Financial Services (DFS) officially published a proposed amendment (the proposed amendment) to its Part 500 Cybersecurity Rules (the regulation).[1] The publication in the state register follows a prior informal release of a draft version of the amendment on July 29, 2022 and included a few revisions to definitions created by the initial draft.[2] If adopted, the proposed amendment would impose heightened cybersecurity obligations on large financial institutions—dubbed "Class A Companies" under the amendment—and would impose some new requirements on all entities subject to DFS' cybersecurity rules.

The public comment period for the proposed amendment began on November 9, 2022 and extends for 60 days until January 9, 2023. **The Council is considering filing comments and member input on proposed amendment is necessary to inform any such comments.** We have included Council summaries of earlier versions of the Part 500 rules for reference.

As discussed in further detail in the Analysis below, the proposed amendment would make the following changes to the Part 500 Cybersecurity Rules:

New "Class A" Company Requirements

The proposed amendment would create a new group of entities called **Class A companies**, defined as *covered entities with at least $20,000,000 in gross annual revenue in each of the last two fiscal years from operations of the covered entity and its affiliates in the state, and: (1) over 2,000 employees averaged over the last two fiscal years or (2) over $1 billion in gross annual revenue in each of the last two fiscal years from operations of the covered entity and all of its*

[1] 44 N.Y. Reg. 26 (Nov. 9, 2022).
[2] The published version of the proposed amendment includes two notable changes as compared to the draft version: (1) the definition of Class A companies is changed, requiring an entity to have at least $20,000,000 in gross annual revenue in each of the past two fiscal years from operations of the covered entity and its affiliates in the state, in addition to either over 2,000 employees averaged over the last two fiscal years, or over $1 billion in gross annual revenue in each of the last two fiscal years from operations of the covered entity and all of its affiliates; and (2) Class A companies are not required to conduct weekly system reviews.

affiliates.[3] The proposed amendment would impose the following new requirements on Class A companies:

- Class A companies must secure annual independent audits of their cybersecurity programs;
- Class A companies must have external experts conduct a risk assessment every three years, in addition to implementing risk assessment processes.

New Requirements for All Entities

The proposed amendment would impose the following new requirements on ***all*** Council members licensed in the State of New York[4]:

- All covered entities must obtain annual approval of their written cybersecurity policy by their Board of Directors (or equivalent body);
- All covered entities must institute a process for identifying cybersecurity risks and update that process annually;
- All covered entities must annually submit written notice of compliance or non-compliance with the regulation.

Broadening of "Exempt Entities"

The proposed amendment would broaden the subgroup of small covered entities that are exempt from certain sections of the regulation.[5] Under the proposed amendment, covered entities would be exempt if they have:

(1) fewer than **twenty** employees and independent contractors of the entity, or affiliates of the entity who meet certain criteria (increased from ten employees in the current rule);
(2) less than **$5 million** in gross annual revenue in each of the last three fiscal years (unchanged from $5 million in the current rule); or
(3) less than **$15 million** in year-end total assets (increased from less than $10 million in the current rule)[6]

New Requirements for Non-Exempt Entities

The proposed amendment would impose the following new requirements that only apply to ***non-exempt*** covered entities, including Class A companies. The requirements do not apply to entities that qualify for "exempt entity" status, discussed above. All non-exempt covered entities must:

- Report any material cybersecurity issues to their Board of Directors (or equivalent body);
- Conduct annual testing of their information systems.

[3] By definition Class A companies would not fall into the limited exemption discussed below.
[4] These requirements apply to all covered entities, including Class A companies and regardless of "exempt" status under § 500.19.
[5] Exempt from §§ 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16.
[6] §§ 500.19(a)(1)-(3).

Summary of New Requirements Under the Proposed Amendment

1. Class A Companies (§§ 500.01, 500.02)

The regulation defines a *covered entity* as any person operating or required to operate under a license, registration, or similar authorization under the New York state Banking Law, Insurance Law, or Financial Services Law.[7] The proposed amendment would create a new subgroup of covered entities called *Class A companies*, meaning covered entities with a least $20,000,000 in gross annual revenue in each of the last two fiscal years from operations of the covered entity and its affiliates in the state, and (1) over 2,000 employees averaged over the last two fiscal years, or (2) over $1 billion in gross annual revenue in each of the last two fiscal years from operations of the covered entity and all of its affiliates.[8] Some new provisions in the proposed amendment would apply specifically to Class A companies.

The proposed amendment would require Class A companies to conduct an annual independent audit of their cybersecurity programs.[9] It would define *independent audit* as an audit conducted by external auditors not influenced by the covered entities being audited.[10]

2. Exempt Entities (§ 500.19)

The regulation would exempt a subgroup of small covered entities from Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.2, 500.14, 500.15, and 500.16.[11] Currently, the regulation exempts covered entities with:

(1) fewer than ten employees and independent contractors of the entity, or affiliates of the entity who meet certain criteria,
(2) less than $5 million in gross annual revenue in each of the last three fiscal years, or
(3) less than $10 million in year-end total assets.

The proposed amendment would expand the exempt entities subgroup by exempting covered entities with:

(1) fewer than **twenty** employees and independent contractors of the entity, and affiliates of the entity who meet certain criteria,
(2) less than **$5 million** in gross annual revenue in each of the last three fiscal years, or
(3) less than **$15 million** in year-end total assets.

Covered entities that *do not* meet these updated requirements are referred to below as "non-exempt" entities.

---

[7] § 500.1(d).
[8] § 500.1(c). The draft version of the proposed amendment defined Class A companies as covered entities with either over 2,000 employees, or over $1 billion in average gross annual revenue in the past three fiscal years from operations of the covered entity and all of its affiliates.
[9] § 500.2(c).
[10] § 500.1(f).
[11] § 500.19.

3. **Written Policies & Reporting** (§§ 500.03, 500.04, 500.16)

   a. ***Requirements Applicable to All Covered Entities***

All covered entities would be required to have their written cybersecurity policies approved at least annually by a Board of Directors (or equivalent governing body), who would be required to have sufficient expertise and knowledge to oversee cyber risk.[12]

   b. ***Requirements Applicable Only to Non-Exempt Covered Entities***

The chief information security officer (CISO) of any non-exempt covered entity would be required to have adequate independence and authority to ensure that cyber risks are managed, and would be required to report material cybersecurity issues to the governing body in a timely manner.[13] All non-exempt covered entities would also be required to establish written plans for incident response, business continuity, and disaster recovery, to be periodically tested.[14]

4. **Information Systems Testing** (§§ 500.05)

   a. ***Requirements Applicable Only to Non-Exempt Covered Entities***

The proposed amendment would require non-exempt covered entities to conduct testing on their information systems at least annually, have a vulnerability monitoring process in place, and to report material gaps found in testing to their governing bodies.[15]

5. **Risk Assessment** (§§ 500.07, 500.09)

   a. ***Requirements Applicable to All Covered Entities***

The regulation would require all covered entities to conduct periodic risk assessments of information systems. The proposed amendment would define *risk assessment* as the process by a covered entity of identifying cybersecurity risks, as specifically applicable to the entity.[16] As part of the risk assessment, covered entities would be required to limit user access privileges and functions to those necessary to perform the user's job, and to periodically review those privileges and remove access that is no longer necessary.[17] The proposed amendment would require the risk assessment to be updated at least annually, and would additionally require covered entities to conduct impact assessments following a material change in the entity's cyber risk.[18]

   b. ***Requirements Applicable Only to Class A Companies***

---

[12] § 500.3.
[13] § 500.4(c).
[14] §§ 500.16.
[15] §§ 500.5(a). The draft version of the proposed amendment required Class A companies to conduct weekly systemic scans, but this provision is *not* included in the published version of the amendment.
[16] § 500.1(n).
[17] § 500.7(a).
[18] § 500.9(c).

Further, Class A companies would be required to have external experts conduct a risk assessment at least once every three years.[19]

6. Notice Requirements (Apply to All Covered Entities) (§§ 500.17)

The proposed amendment would modify the regulation's notice requirement as follows – each covered entity would be required to annually submit by April 15 one of two electronic written notices: (1) a written certification that the covered entity complied with the regulation, or (2) a written acknowledgement that the entity did not fully comply with requirements of the regulation and identifying the provisions that the entity has not fully complied with and the extent of such noncompliance.[20] Additionally, the entity would be required to thoroughly document the remedial efforts planned and a timeline of such efforts.[21]

Covered entities would also be required to provide the superintendent notice and explanation of an extortion payment within 24 hours of such payment and, within 30 days, a written description of the reasons the payment was necessary, alternatives considered, and what due diligence was performed.[22]

7. Exemptions & Enforcement (Apply to All Covered Entities) (§§ 500.11, 500.20)

The regulation requires that covered entities have written policies to ensure security of information systems accessible to third party service providers.[23] The proposed amendment includes a technical revision to remove a duplicative exemption from this third party provider requirement for agents and employees of covered entities. Specifically, the amendment would eliminate a limited exemption that previously allowed an agent, employee, representative, or designee of a covered entity that is itself a covered entity to not develop their own third party information security policy, if the agent, employee, representative, or designee followed the policy of the relevant covered entity.[24] This provision provided a narrow exemption that is already covered under an existing exemption for agents and employees that would be untouched by the proposed amendment (§ 500.19(b)).[25] Therefore the removal in the proposed amendment is a technical revision not intended to effectuate a material change.

Lastly, the amendment would clarify the process for calculating penalties, including the factors DFS must consider when making its assessment.[26] Notably, an entity's failure to comply with any part of the regulations for more than 24 hours or failure to prevent unauthorized access to nonpublic information on account of such noncompliance would constitute a violation.[27] In assessing the penalty, DFS would take into account a variety of factors including the entity's good faith, whether the conduct was unintentional, reckless, or deliberate, whether the violation

[19] § 500.9(d).
[20] § 500.17(b).
[21] § 500.17(b).
[22] § 500.17(c).
[23] § 500.11(a).
[24] § 500.11(c).
[25] § 500.19(b).
[26] § 500.20.
[27] § 500.20(b).

was a result of a failure to remedy previous matters requiring attention, and the entity's prior violation history, among others.[28]

8. Time Period for Compliance (Apply to All Covered Entities) (§§ 500.21, 500.22)

Amendments to the regulation would become effective upon publication of the Notice of Adoption in the State Register.[29] Under the proposed amendment, covered entities would have 180 days from the effective date of an amendment to comply with new requirements under that amendment, unless otherwise specified.[30] Notably, the above discussed notice requirement as amended would have a different transitional period under the proposed amendment – covered entities would have 30 days from the effective date of this notice requirement (found in Section 500.17) to comply.[31]

[28] § 500.20(c).
[29] § 500.21(b).
[30] § 500.22(c).
[31] § 500.22(d)(2).