NYDFS Publishes Official Amendments to Its Cybersecurity Regulation (Part 2) – Answers to the Top Questions from Our Webcast

November 30, 2022

On November 9, 2022, the New York Department of Financial Services (the "NYDFS") announced the publication of the official proposed amendments to its 2017 Cybersecurity Regulation 23 NYCRR 500 (the "Proposed Amendments"). The 60-day public comment period to the Proposed Amendments ends on January 9, 2023. We provided our initial thoughts on the Proposed Amendments in a blog post, and then held a webcast on November 18, 2022, during which we received several questions that we did not have time to answer. Below are those questions, along with answers that illustrate some of the remaining ambiguities that the Proposed Amendments present, which hopefully will be resolved during the comment process.

Question #1: Are affiliates of covered entities, which are not themselves covered entities, subject to the new requirements set forth in the Proposed Amendments?

Technically, no. Practically, maybe. We received several versions of this question. By their terms, the Proposed Amendments do not draw in affiliates of covered entities. But as more cybersecurity requirements are placed on covered entities, they are more likely to rely on outside assistance for compliance. To the extent that covered entities rely on noncovered entity affiliate(s) for compliance with any of the obligations created by the Proposed Amendments (e.g., controls for privileged accounts, endpoint detection, audits, business continuity planning, asset inventory, etc.), those affiliates may fall under the scope of NYDFS scrutiny for Part 500 compliance. The NYDFS addresses this issue on its Cybersecurity Resource Center, which includes this FAQ:

> ***6. May a Covered Entity adopt portions of an Affiliate's cybersecurity program without adopting all of it?***
> *A Covered Entity may adopt an Affiliate's cybersecurity program in whole or in part as provided for in Part 500.2(c), as long as the Covered Entity's overall cybersecurity program meets all requirements of 23 NYCRR Part 500. The Covered Entity remains responsible for full compliance with the requirements of 23 NYCRR Part 500. To the extent a Covered Entity relies on an Affiliate's cybersecurity program in whole or in part, that program must be made available for examination by the Department.*

To reinforce this point, the Proposed Amendments add the underlined language to Part 500.2(e):

> All documentation and information relevant to the covered entity's cybersecurity program, including the relevant and applicable provisions of a cybersecurity program maintained by an affiliate and adopted by the covered entity, shall be made available to the superintendent upon request.

Additionally, non-covered-entity affiliates may fall under NYDFS scrutiny to the extent that they may pose a risk to the cybersecurity of covered entities, as noted in this NYDFS FAQ:

> ***12. How must a Covered Entity address cybersecurity issues with respect to its subsidiaries and other affiliates?***
> *When a subsidiary or other affiliate of a Covered Entity presents risks to the Covered Entity's Information Systems or the Nonpublic Information stored on those Information Systems, those risks must be evaluated and addressed in the Covered Entity's Risk Assessment, cybersecurity program and cybersecurity policies (see 23 NYCRR Sections 500.9, 500.2 and 500.3, respectively). Other regulatory requirements may also apply, depending on the individual facts and circumstances.*

Question #2: Will the Class A requirements apply to a small NY branch of a foreign banking organization?

Yes, if the small NY branch (the covered entity) meets the definition of a Class A company due to its relationship with the foreign banking organization, either alone or when combined with its affiliates. But the Proposed Amendments revised the pre-proposal by including a newly added threshold requirement to qualify for Class A status:

- The NY branch and affiliates have at least $20 million in gross annual revenue for each of the last two years from their operations in New York, and:

  (1) over 2,000 employees averaged over the last two fiscal years, including those of both the covered entity and all of its affiliates no matter where located; or
  (2) over $1 billion in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates.

Question #3: What cybersecurity expertise is required for the board? If the board lacks such expertise, can it receive guidance or training from internal resources?

Unclear. The Proposed Amendments add a requirement to Part 500.4 that, to the extent that a covered entity has a board of directors or equivalent, "the board or an appropriate committee thereof shall . . . have sufficient expertise and knowledge, or be advised by

persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management." It is unclear what level of experience or expertise will be viewed as sufficient to meet this standard, and whether it is sufficient for that expertise to reside in a single board member. What is clear is that the board is being asked to not just oversee the cyber program, but also receive updates on material issues in vulnerability testing. Providing effective oversight of material issues in vulnerability testing will require more than passing knowledge of cybersecurity.

If a covered entity is unsure whether its board or equivalent governing body has the requisite cybersecurity expertise, it should consider making cybersecurity advisory services available to the board. The Proposed Amendments do not specify that such advisers must be external to the covered entity, but given that the goal of the advice would be to assist the board in exercising effective oversight over cybersecurity risk management, it would be better if the advisers were not involved in the covered entity's cybersecurity program. This means either external advisers or experts from a parent or affiliate of the covered entity that are not involved in the covered entity's compliance with Part 500 would be preferable.

Question #4: What is supposed to be covered by the annual independent audit for Class A companies?

Unclear. Part 500.2 is titled "Cybersecurity Program" and provides that "[e]ach covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information stored on those information systems." The Proposed Amendments add a new subsection (c) to that section which provides that "Class A companies shall conduct an independent audit of their cybersecurity programs at least annually." The term "independent audit" is defined as "an audit conducted by external auditors free to make decisions not influenced by the covered entities being audited or by its owners, managers or employees."

There is some ambiguity as to whether such an audit is supposed to (1) cover compliance with 500.2 and any other required elements of a cybersecurity program to the extent not included in one of the Part 500.2(b) enumerated functions, (2) cover compliance with all of Part 500, including, for example, the governance requirements in Part 500.4, or (3) be a different kind of cybersecurity audit such as a SOC 2 Type 1 or Type 2.

We believe that option 1 is the most logical reading of the provision, with option 2 a close second, but hopefully, this issue will be clarified through the comment process. If the NYDFS had contemplated Option 2 in its Proposed Amendments, presumably it would have used a similar formulation as in Section 500.17, which requires the notice of

compliance to cover "the requirements set forth in this Part." In addition, whether employees of an affiliate could conduct an "independent audit" is also unclear and should be resolved through the comment process.

Question #5: Are the business continuity and disaster recovery ("BCDR") plans in 500.16 limited to cyber events, or does it cover all BCDR issues, including power outages, pandemics, etc.? In other words, is the CISO now responsible for all BCDR?

Unclear. Under Part 500.4, the CISO is responsible for overseeing and implementing a covered entity's cybersecurity program and enforcing its cybersecurity policy. Part 500.16 starts with "[a]s part of its cybersecurity program, each covered entity shall establish written plans that contain proactive measures to investigate and mitigate disruptive events and ensure operational resilience, including but not limited to incident response, business continuity and disaster recovery plans." The Proposed Amendments provide in Part 500.16(b)(2) that the BCDR plans "shall be reasonably designed to ensure the availability and functionality of the covered entity's services and protect the covered entity's personnel, assets and nonpublic information in the event of an emergency or other disruption to its normal business activity."

One reasonable reading of these provisions is that the CISO is responsible for overseeing and implementing all BCDR plans, including those that are not tied to cyber events, but this is another issue that will hopefully be resolved through the comment process.

Question #6: Do the Proposed Amendments lower the threshold for notification to the NYDFS for vendor breaches?

Unclear. Part 500.17 currently provides that notification of a cybersecurity event must be made to the NYDFS if (a) notification was required to any other government agency, or (b) it was reasonably likely to materially harm any material part of the covered entity's normal operations. The term "cybersecurity event" is defined in Part 500.1 as "any act or attempt . . . to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system."

The Proposed Amendments added three new notification triggers: (1) an unauthorized user gaining access to a privileged account; (2) deployment of ransomware within a material part of a covered entity's information systems; and (3) a covered entity is affected by a cybersecurity event at a third party service provider. In context, one would assume that the addition of the subsection on third party service provider breaches was to clarify that notification events that occur on third party information systems can still be notification events for the covered entity.

So, for example, if (i) a covered entity stores sensitive customer data with a third party, and (ii) that third party experiences a cybersecurity event that requires the covered entity to notify regulators in a different state, the inclusion of Part 500.17(3) in the Proposed Amendments was designed to make clear that the NYDFS must be notified in that situation, even though the cybersecurity event did not occur on the covered entity's information systems. But, as drafted, Part 500.17(3) appears broader, and does not seem to condition notification of third party cybersecurity events to NYDFS on either a separate notification obligation or materiality, and therefore could be read to require notification to the NYDFS of any cybersecurity event that occurs at a covered entity's third party service provider, so long as it affects the covered entity. Again, this is an ambiguity that will hopefully be resolved through the comment process.

Question #7: Do the proposed changes to 500.17(b) and 500.20(b) mean that any 24-hour period of noncompliance with any provision of Part 500 will prevent a company from certifying to compliance as part of its annual certification?

Unclear. Part 500.17(b) currently requires a covered entity to certify that, for the prior calendar year, it "*is in compliance* with the requirements set forth in this Part." Under the Proposed Amendments, a covered entity must certify that, "for the prior calendar year, [it] *complied* with the requirements set forth in this Part," or the covered entity must submit a written acknowledgement noting that it "did not fully comply with all the requirements of this Part" and specifically identify its compliance gaps and remediation roadmap. The new Part 500.20(b) states that "the failure to comply for any 24-hour period with any section of this Part" is a violation.

Taken together, one could argue that under the Proposed Amendments, any 24-hour gap in compliance in the previous calendar year with any provision of Part 500 would prevent certification of compliance, and instead requires a written acknowledgement of noncompliance. This could mean that few covered entities will be able to certify, considering how common it is to have short gaps in compliance with at least one provision of Part 500. Again, this may not have been what the NYDFS intended with the Proposed Amendments and hopefully will be resolved in the comment process.

The authors would like to thank Debevoise Law Clerk Ned Terrace for his contribution to this blog post.

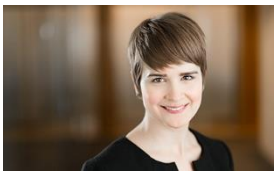
To subscribe to the Data Blog, please click here.

* * *

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com



Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

SAN FRANCISCO

Mengyi Xu
mxu@debevoise.com