NYDFS Proposes Significant Changes to Its Cybersecurity Rules (Part 2) – Answers to the Top 10 Questions from Our Webcast

August 8, 2022

On July 29, 2022, the New York Department of Financial Services ("NYDFS") released Draft Amendments to its Part 500 Cybersecurity Rules. We provided our initial thoughts on the Draft Amendments in a blog post, and then had a webcast on August 5, 2022, during which we received dozens of questions, some of which we did not have time to answer. In this update, we answer some of the questions we received in connection with our webcast and our initial blog post, which discussed the six categories of changes to the NYDFS's Part 500 Cybersecurity Rules: Obligations for Larger (Class A) Companies, Governance, Risk Assessments, Technical Requirements, Notification Obligations, and Penalties.

The Scope of Class A Companies and Affiliates

As we wrote in our previous blog post, the Draft Amendments create a category of "Class A" companies, which are covered entities with over 2,000 employees (including those of affiliates no matter where located) or over $1 billion in gross annual revenues averaged over the last three years from all business operations of the company and its affiliates. Class A companies are subject to several additional cybersecurity obligations, including:

- **Audits**. An independent audit of the company's cybersecurity program must be conducted at least annually.

- **Vulnerability assessments**. Systematic scans or reviews of information systems must be conducted at least weekly, and any material gaps found during testing must be documented and reported to the board and senior management.

- **Password controls**. A password vaulting solution must be implemented for privileged accounts, along with an automated method of blocking commonly used passwords.

- **Monitoring**. An endpoint detection and response solution must be implemented to monitor anomalous activity, including lateral movement, as well as centralized logging and security event alerting.

We received numerous questions about the relationships between bank holding companies and/or foreign companies and their covered-entity subsidiaries. The general principles governing these issues are unchanged in the Draft Amendments. Covered entities are responsible for their cybersecurity programs. Even when they rely on the cybersecurity programs of their parent companies or affiliates, the responsibility for compliance attaches to the covered entity. NYDFS covers these issues in their FAQs. See FAQ 13 (discussing Bank Holding Companies); FAQ 5 (discussing branches of foreign banks); FAQ 6 (discussing use of an affiliates program); and FAQ 7 (discussing reliance on the CISO of a parent company or affiliate).

Question 1: Will the Class A requirements apply to a small NY branch of a large overseas bank?

Yes, assuming the large overseas affiliate bank of the small NY branch (the covered entity) meets the above definition of a Class A company, either alone or when combined with its affiliates. The definition of Class A companies specifically includes language to this effect; for example, in discussing the 2,000 employees, it states "including those of both the covered entity and all of its affiliates no matter where located" (emphasis added).

Question 2: Under what circumstances will affiliates of a covered entity be subject to the Draft Amendments?

As we discussed during the Webcast, to the extent the covered entity relies on an affiliate for the policies, controls, or personnel necessary for compliance with the Draft Amendments, it risks subjecting that affiliate to the scrutiny of the NYDFS with respect to those policies, controls, or personnel. Indeed, the NYDFS makes this point on its Cybersecurity Resource Center, which includes an FAQ that states "only the Information Systems supporting the [covered entity] branch, agency or representative office, and the Nonpublic Information of the branch, agency or representative office are subject to the applicable requirements of 23 NYCRR Part 500, whether through the branch's, agency's, or representative office's development and implementation of its own cybersecurity program *or through the adoption of an Affiliate's cybersecurity program*" (emphasis added).

Question 3: Could a small covered entity that would, on its own, qualify for exemptions from many of the Part 500 Requirements (e.g., because it has fewer than 20 employees)

still be considered a Class A company if it has a large affiliate that qualifies for Class A status?

It appears so. First, under the Draft Amendments, some very small covered entities will no longer qualify for the exemptions in Part 500.19 because of new changes. For example, those exemptions no longer apply if the covered entity has 20 or more employees and independent contractors who work for the covered entity or who work for an affiliate of the covered entity and whose work is located in New York state. The exemptions also do not apply if 20 or more employees and independent contractors work for an affiliate of the covered entity and are responsible for the business of the covered entity, regardless of their location. So, the small covered entity would truly need to stand alone from its larger affiliates to qualify for an exemption.

Second, even in instances where a small covered entity does qualify for the exemptions in Part 500.19, that small covered entity is still a Class A company if it has an affiliate that qualifies as a Class A company. Although Part 500.19(a) would exempt such an entity from many of the Part 500 obligations, it would still be subject to the requirements of 500.7 (access privileges, including the requirements that Class A companies have password vaulting), 500.9 (risk assessments, including the requirement that Class A companies use external experts at least once every three years), 500.11 (third-party service providers), and 500.13 (asset inventory). Read literally, very small covered entities that qualify for the exemption under Part 500.19(a)(1) could nonetheless be subject to some of the new requirements for Class A companies. This issue is therefore worth raising through the comment process, as that consequence may not have been the intended result of the Draft Amendments.

Question 4: Is the addition of "including entities that are also regulated by other government agencies" a significant expansion of the definition of "covered entity" to financial institutions that are not currently covered by Part 500?

No. The definition of "covered entity" remains the same: any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the [New York] Banking Law, the Insurance Law or the Financial Services Law, *including entities that are also regulated by other government agencies*. The inclusion of the word "also" in that added italicized text indicates that this amendment is designed only to clarify that entities that meet the existing definition of covered entities are not exempt from compliance merely because they are also regulated by other government agencies. Accordingly, the Draft Amendments will only apply to financial companies outside of New York state to the extent that these entities meet the definition of "covered entity," subject to the considerations discussed above regarding affiliates of covered entities.

Question 5: How will these new rules impact non-covered entities?

When the NYDFS issued the original Part 500 cybersecurity rules in 2017, the rules were precedent setting. The National Association of Insurance Commissioners (NAIC) later created a model act that largely tracked Part 500; other regulators have adopted similar cybersecurity regulatory frameworks. Consistent with past practice, the Draft Amendments will likely influence other regulators and raise the bar for their cyber regulations.

Another likely impact of the Draft Amendments is that once hundreds of covered entities are able to certify their compliance with the new requirements, the bar has arguably been raised as to what constitutes "industry best practices" or "reasonable security" for financial institutions. While not every new measure in the Draft Amendments will become part of the standards expected by other regulators (or judges), the overall effect is likely to be a further raising of expectations for cybersecurity.

In addition, some affiliates of covered entities will likely adopt the same enhancements that the Draft Amendments require for their covered entities in order to maintain a single enterprise-wide approach for cybersecurity.

Question 6: Should covered entities try to comply with the Class A requirements if they are not Class A entities?

The Class A requirements in the Draft Amendments are clearly designed to reduce cyber risk. So, if covered entities that are not subject to the Class A requirements can easily conduct annual independent audits and weekly vulnerability scans, implement a password vaulting solution, and deploy an endpoint detection and response solution, those enhancements will likely reduce their overall cybersecurity risk. But each covered entity must conduct a risk assessment and decide which non-mandatory measures are most likely to be effective and whether the time, money, and effort of implementing those enhancements are worthwhile in light of the risk and other existing controls. Many businesses will reasonably decide to wait to implement the requirements for Class A companies until they are required to do so by regulation, or they are considered to be "reasonable cybersecurity" measures for companies of their size in their sector.

Technical Amendments

Question 7: What are the criteria for the annual audits and risk assessments of Class A companies? Would assessments under the FFIEC Cyber Assessment Tool, the CRI Profile, and the NIST Cybersecurity Framework be sufficient?

The Draft Amendments do not specify any particular criteria for the audits, aside from requiring that they be independent and that Class A companies conduct the audits annually. However, the NYDFS does specify that the audits can be conducted by an internal auditing body and need not be carried out by external auditors.

The Draft Amendments do provide new specifications for risk assessments. In public presentations, the NYDFS has commented that they have seen risk assessments that appear to be cookie-cutter reviews, with only the particular name of the covered entity changed from one risk assessment to the next. The new specifications appear designed to ensure that the risk assessments are tailed to "the specific circumstances of the covered entity." Indeed, proposed section 500.1(n) lists the elements that a risk assessment must consider, including size, staffing, governance, services, products, vendors, and locations, among others. The risk assessments must also incorporate threat and vulnerability analysis.

Previously, in its FAQ, the NYDFS explained that it is agnostic as to which framework is used in risk assessments. Presumably, this will continue to be the case, although it cited the FFIEC, CRI, and NIST frameworks as examples of "widely used frameworks."

Notice to the NYDFS

Question 8: Covered entities will be required to notify the NYDFS where an unauthorized user gains access to a privileged account. Does this only apply to malicious actors, or does it also apply to employees or contractors who exceed their authority or where there has been a configuration error?

The new proposed notification requirement pertaining to unauthorized access to privileged accounts is triggered by "cybersecurity events," which are in turn defined to cover malicious acts (i.e., acts or attempts to gain unauthorized access to, disrupt or misuse any information system or information stored on such information system). An unauthorized access to a privileged account where no cybersecurity event occurs should therefore not, by itself, trigger a notification requirement. Although an insider could trigger a cybersecurity event by deliberately gaining unauthorized access to a privileged account, innocent unauthorized access (e.g., due to a configuration error), should not qualify as a notification trigger, but this issue is another point that may warrant clarification through the comment process.

Question 9: If an extortion payment is made in connection with a cybersecurity event, the covered entity must provide the NYDFS, within 30 days, a written description of the reasons payment was necessary, alternatives to payment considered, diligence performed to find alternatives to payment, and diligence performed to ensure

compliance with applicable regulations. How can a covered entity comply with this requirement without waiving privilege?

As we discussed during the Webcast, in these circumstances, covered entities will have to share non-privileged facts with the NYDFS sufficient to satisfy this obligation. For example, facts such as: backups were encrypted, the threat actor was not on any OFAC sanctions list, the FBI was consulted, the sensitivity of the data that was stolen, etc., are not privileged. These circumstances may merit the preparation of a non-privileged written report, in addition to any written report over which the covered entity would assert privilege.

Question 10: To the extent that it was not in full compliance with Part 500 in the prior calendar year, a covered entity must identify all provisions that it has not fully complied with and describes the nature and extent of such noncompliance, and identify all areas, systems, and processes that require material improvement, updating, or redesign. For security reasons, this is not normally information that we share in writing outside the organization.

This is another good issue to raise during the Comment Period. In the past, industry has worked with regulators to find secure ways to share such information, including, if needed, a secure transmittal. Regulators understand the risks of storing such information on their systems, and trade associations are also familiar with these issues and may already be thinking of recommending best practices to the NYDFS.

The Comment Period

In the lead up to the adoption of the original Part 500, the NYDFS was very open to industry feedback and will likely take comments very seriously in finalizing the Draft Amendments.

The short pre-proposal comment period has been extended to August 18, 2022. We anticipate that the NYDFS will publish a substantially similar version of the Draft Amendments in the coming weeks, which will start a 60-day comment period. If adopted, most of the Draft Amendments would take effect 180 days from the date of adoption. The expanded notification requirements and the changes to annual notice of certification would, however, take effect 30 days after adoption. Also, many of the technology-related amendments (e.g., new requirements for passwords, access controls, and endpoint detection solutions) would take effect one year after adoption.

We are gathering additional questions and concerns in anticipation of filing comments. Please feel free to share any thoughts you have about the Draft Amendments by emailing any of the authors.

To subscribe to the Data Blog, please click here.

* * *

NEW YORK

Eric Dinallo
edinallo@debevoise.com

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Caroline Novogrod Swett
cnswett@debevoise.com

Charu Chandrasekhar
cchandrasekha@debevoise.com

WASHINGTON, DC

Luke Dembosky
ldembosky@debevoise.com