Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Upcoming February and March Deadlines Under New York DFS Cybersecurity Regulation, Including New Third-Party Service Provider Requirements

January 28, 2019

This client alert will briefly outline key upcoming deadlines under the New York State Department of Financial Services (DFS) Cybersecurity Regulation (the "Regulation"). These include annual filing deadlines coming up in February, as well as new third-party service provider requirements that will go into effect on March 1, 2019.

I. February Filing Deadlines for Certificates of Compliance and Notices of Exemption

Certificates of Compliance – Prior to **February 15, 2019**, all regulated entities and licensed persons must file a certificate of compliance with DFS, confirming their compliance with the Regulation for the calendar year 2018. DFS has issued helpful instructions for completing the certificate of compliance, which are available here. Covered entities or their affiliates, which are eligible for a limited exemption under Section 500.19(a) (i.e., entities with fewer than 10 employees in New York, less than $5 million in gross annual revenue in the last three years from New York business or less than $10 million in year-end total assets) must still comply with multiple provisions of the Regulation. Those entities may want to file both a notice of exemption (further discussed below) and a certificate of compliance demonstrating their compliance with the sections of the Regulation that continue to apply even after application of the limited exemption.

Notices of Exemption – Prior to **February 15, 2019**, covered entities that meet the requirements for exemptions in Section 500.19 must file a notice of exemption. Exemptions filed in 2017 and 2018 have expired, and any exempt entities that previously filed notices of exemption should file new notices. DFS has issued helpful instructions for completing the notice and for determining the applicability of various exemptions, which are available here. As noted above, covered entities that are eligible for the limited exemptions in Section 500.19(a) may want to submit both a notice of exemption and a certificate of compliance.

Contact

Natasha Kohne
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle Reed
mreed@akingump.com
Dallas
+1 214.969.2713

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Diana Schaffner
dschaffner@akingump.com
San Francisco
+1 415.765.9507

Tylor Dominguez
tdominguez@akingump.com
San Francisco
+1 415.765.9543

II. Third-Party Service Provider Requirements Go Into Effect on March 1, 2019

On March 1, 2019, Section 500.11, which relates to third-party service providers, comes into force. This is the last section of the Regulation to take effect. Covered entities will have to certify their compliance with Section 500.11 for the first time as part of their February 2020 submissions indicating their compliance with the Regulation for the calendar year 2019. Covered entities that qualify for a limited exception pursuant to Section 500.19(a) must still comply with Section 500.11, among other sections.

Section 500.11 requires all covered entities to have written policies and procedures that are designed to ensure the security of their information systems and any nonpublic information that is accessible to, or held by, third-party service providers. The policies and procedures must be based on each covered entity's own previously conducted risk assessment and should address the following topics, if applicable:

1. The identification and risk assessment of third-party service providers
2. Minimum cybersecurity practices that are required to be met by third-party service providers
3. Due diligence processes that are used to evaluate the adequacy of cybersecurity practices of third-party service providers
4. Periodic assessments of third-party service providers based on the risk that they present and the continued adequacy of their cybersecurity practices.

The policies and procedures also must include guidelines for due diligence and/or contractual protections relating to third-party service providers. The guidelines should address:

1. Third-party service providers' policies and procedures for access controls, including their use of multifactor authentication, to limit access to relevant information systems or nonpublic information
2. Third-party service providers' policies and procedures for use of encryption to protect nonpublic information in transit
3. Notice to be provided to the covered entity should a cybersecurity event occur that directly impacts the covered entity's information systems or its nonpublic information being held by the third-party service provider
4. Representations and warranties addressing the third-party service provider's cybersecurity policies and procedures that relate to the security of the covered entity's information systems or nonpublic information.

Third-party service provider risks remain a key issue of interest to a variety of regulators, including the Securities and Exchange Commission, as well as DFS. Adopting a strong third-party service provider policy can help companies to minimize their vendor risks. Doing so may also support later claims that the company followed "reasonable security" measures should a cybersecurity event occur, and thus reduce some litigation and regulatory risks.