Upcoming New York State Cybersecurity Regulation Deadlines

Skadden

02 / 07 / 19

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

Four Times Square
New York, NY 10036
212.735.3000

As a reminder, entities covered by the New York State Department of Financial Services' (NYSDFS) Cybersecurity Regulations (23 NYCRR Part 500) (Cybersecurity Regulations) are required to submit their annual certification of compliance for calendar year 2018 no later than February 15, 2019. In addition, the last transitional period of the regulations will end on March 1, 2019, after which covered entities will need to comply with the third-party service provider provisions.

What Is Required for the Annual Certification?

The certification requires a member of the board of directors or a senior officer responsible for the management, operations, security, information systems, compliance and/or risk of the entity to attest that the board of directors or the senior officer has reviewed the entity's policies and documentation required under the Cybersecurity Regulations and, to the best of their knowledge, the entity's cybersecurity program was in compliance with the Cybersecurity Regulations' requirements during the past calendar year. Instructions for filing the certification with NYSDFS are available here.

Importantly, if during its annual certification review of the policies and procedures required by the Cybersecurity Regulations, a covered entity identifies areas, systems or processes that require "material improvement, updating or redesign," then the entity must document the "identification and the remedial efforts planned and underway to address such areas, systems or processes" and maintain such documentation for potential inspection or review by NYSDFS.

What Requirements Go Into Effect on March 1, 2019?

March 1, 2019, ends the final transitional period of the Cybersecurity Regulations, after which covered entities must comply with all of the requirements. As of this date, covered entities must have written policies and procedures in place that are designed to ensure the security of its information and systems accessible to, or held by, third-party service providers. These policies and procedures must include: (1) the identification and risk assessment of all providers; (2) minimum cybersecurity practices required to be met by the providers in order to do business with the covered entity, including their use of access controls and encryption of data in transit and at rest; (3) due diligence processes for evaluating the adequacy of providers' cybersecurity practices; and (4) the periodic assessment of the providers' cybersecurity practices. Covered entities must also have contractual provisions in their agreements with their service providers regarding the security of the covered entity's information and systems, and requiring that the providers provide notice to the covered entity in the event of a security incident involving its information or systems.

Given the delayed implementation of these requirements, covered entities do not need to include compliance with the third-party service provider requirements in their 2018 certification.

Should We Expect Robust Enforcement by NYSDFS?

To date, NYSDFS has been active in the use of its cybersecurity regulatory authority, including focusing on cybersecurity preparedness in their examinations of financial institutions. Further, in a December 2018 memorandum reviewing the first two years

Upcoming New York State Cybersecurity Regulation Deadlines

of the Cybersecurity Regulations, Maria T. Vullo, who until recently was the NYSDFS superintendent, noted that the department's enforcement of the regulations will include regular and targeted examinations, and that the department has established internal policies and procedures for reviewing confidential information provided by covered entities. It remains unclear, however, how NYSDFS will enforce the Cybersecurity Regulations and remedy noncompliance, given the novel nature of its implementation.

For more information on the NYSDFS Cybersecurity Regulations, please see our previous client alerts, available here and here, as well as NYSDFS' Cybersecurity Resource Center.

Contacts

Brian D. Christiansen
Partner / Washington, D.C.
202.371.7852
brian.christiansen@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

William J. Sweet, Jr.
Partner / Washington, D.C.
202.371.7030
william.sweet@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Joe Molosky
Associate / Chicago
312.407.0512
joe.molosky@skadden.com