New York DFS Cybersecurity Regulation Update: Lots Left to Do

Authored by: Theodore P. Augustinos

December 2017

This article was reprinted with permission from the December 2017 issue of the Intellectual Property & Technology Law Journal.

Insurance companies and producers, banks, lenders, and others licensed by the New York Department of Financial Services (DFS) have already had to comply with several of the requirements of the new DFS Cybersecurity Regulation, but for most, there's a lot left to do. For the financial services and insurance industries, the Regulation has far reaching implications, affecting many DFS licensees ("Covered Entities") and requiring significant planning and effort from the time of the Regulation's effective date of March 1, 2017 through the last transition date of March 1, 2019 and beyond.

From the time of the Regulation's effective date, Covered Entities needed to take immediate action to meet its various compliance requirements, which started transitioning into to effect on August 28, 2017. Even Covered Entities subject to one of the limited exemptions must satisfy many of the Regulation's new requirements, and even employees, agents and others who are covered by the information security program of an employer or principal had to file for an exemption.

August 28, 2017: Hopefully, you were prepared.

By the first transition date of August 28, 2017, most Covered Entities had to satisfy the following requirements:

- Cybersecurity Program must be maintained;
- Cybersecurity Policy must be drafted and implemented;
- Chief Information Security Officer must be designated (unless subject to a limited exemption);
- Access Privileges must be limited;
- Cybersecurity Personnel must be engaged, trained and updated (unless subject to a limited exemption);
- Incident Response Plan must be drafted and established (unless subject to a limited exemption); and
- Notices to Superintendent of certain cybersecurity incidents will be required.

Are you subject to one of several potential exemptions? You should have filed your Notice by October 30.

As noted above, even Covered Entities subject to one of the limited exemptions, and employees and others, must file a Notice of Exemption, which is due within 30 days after a determination that the exemption applies. DFS initially interpreted this requirement to mean that Covered Entities subject to one of the exemptions at the time of the first transition date (August 28) must have filed by September 27, 2017, but later extended the deadline to October 30.

February 15, 2018: The First Annual Compliance Certificate.

A significant requirement of the Regulation is that a Senior Officer (as defined by the Regulation) or the Board of Directors must, on behalf of the Covered Entity, certify that the Covered Entity is in compliance with all applicable requirements of the Regulation. It is important to note that if a Covered Entity cannot certify that all of the applicable requirements are satisfied, the Covered Entity cannot file the compliance certificate; no exemptions may be taken. (Note that requirements are only covered by the compliance certificate once the applicable transition date has passed.) As the individual or individuals making the certification, which is to be submitted electronically on a prescribed form, will need to be identified, and satisfied that the certificate is truthful, this requirement should be part of the planning starting now, and not left until the deadline.

March 1, 2018: What to Focus on Next?

By the next transition date of March 1, 2018, each Covered Entity will need to have completed its first periodic risk assessment under written policies and procedures, and document its findings. In addition, Covered Entities other than those subject to a limited exemption must meet the following requirements of the Regulation:

- First annual requirement for CISO's report to the Board;
- Continuous monitoring, or periodic penetration testing and vulnerability assessments;

- Multi-factor authentication or risk-based authentication; and
- Cybersecurity awareness training for all personnel.

September 3, 2018: Most of the Rest.

The most of the remaining requirements of the Regulation must be satisfied by September 3, 2018, except the requirement to draft and implement written policies and procedures to manage security risk presented by third party service providers, for which the transition date is March 1, 2019. Covered Entities must, by September 3, 2018, draft and implement policies and procedures limiting the retention of certain data, and providing for its secure disposal. In addition, Covered Entities other than those subject to a limited exemption are required by September 3 with the following requirements:

- Establish and document an audit trail able to recreate material financial transactions and to detect and respond to certain cybersecurity events;
- Draft and implement policies for security of applications used within tech environment;
- Monitor activities of authorized users; and
- Satisfy encryption requirements.

Looking past March 1, 2019: The Last of the Transition Dates is NOT the End of the Project.

Even after the last transition date of March 1, 2019, at which time the third party service provider requirements (as well as all other applicable provisions of the Regulation) will be fully operational, Covered Entities will not be finished with their efforts to comply with the DFS Cybersecurity Regulation. Several requirements of the Regulation will require ongoing, and continuous or periodic, attention, including the requirements for risk assessments, penetration testing and vulnerability assessments, monitoring and training of employees, reports to the Board of Directors, filings of compliance certificates, and notices of certain cybersecurity events.

In addition, it is important to note that several of the policies to be developed and implemented pursuant to the Regulation are to be based on the periodic risk assessment. As the risk assessment is to be conducted periodically, and as the results will change over time, the policies and procedures to be based on the risk assessment will need attention, modification, and refinement on an ongoing basis.

In addition, as evidenced by recent developments by the NAIC to develop a model cybersecurity law based on the DFS Regulation, and by the new effort in Colorado that applies to securities firms, new and additional requirements will certainly be imposed by other regulators and jurisdictions, potentially requiring additional, state-specific attention by Covered Entities licensed in other jurisdictions.

There is still a lot left to do to comply with the New York Department of Financial Services Cybersecurity Regulation, and this is a project that, for most Covered Entities, will not end.

ABOUT THE AUTHOR

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Ted Augustinos is a partner at Locke Lord LLP advising clients in various industries on privacy and data protection, and on a wide variety of transactions, regulatory compliance, and corporate matters.