THE
NATIONAL LAW REVIEW

Developments in New York and Colorado Cybersecurity Regulations

Article By
Gregory Bautista
Jeremy T. Merkel
Wilson Elser Moskowitz Edelman & Dicker LLP
Client Alert

- Communications, Media & Internet
- Colorado
- New York

Friday, August 18, 2017

New York

For the first time since New York's Cybersecurity Regulation (23 NYCRR Part 500) became effective on March 1, 2017, the Department of Financial Services (DFS) has issued **Frequently Asked Questions** to assist Covered Entities in their compliance and provide guidance into the DFS's interpretation and enforcement of its newly adopted regulation.

Since the new Regulation was promulgated, Covered Entities, including banks, financial institutions and insurance companies, have faced uncertainly as to how their compliance will be assessed by DFS. With the Regulation's first deadline for implementation quickly approaching on August 28, 2017, these updated FAQs offer some much needed clarification.

One of the most perplexing aspects of the Regulation is what constitutes a reportable "Cybersecurity Event." DFS recognizes that Covered Entities are regularly subjected to routine and unsuccessful attempts to gain unauthorized access to their information systems and underlying data. In such instances, DFS will defer to the Covered Entity's "appropriate judgment" as to when unsuccessful attacks must be reported. In using their appropriate judgment, Covered Entities should consider whether responding to the attack requires measures beyond those ordinarily taken, or if the risks unique to the Covered Entity would render an otherwise unsuccessful attack particularly significant.

While DFS has stated that it "does not intend to penalize Covered Entities for the exercise of honest, good faith judgment," if the attack is "sufficiently serious to raise a concern," it must be reported no later than 72 hours after determining that a reportable Cybersecurity Event has occurred. At minimum, a Cybersecurity Event is reportable under any of the following circumstances:

- Notice is required to any government body, self-regulatory agency or any other supervisory body (23 NYCRR 500.17(a)(1))
- Notice is required to affected consumers or government agencies under other laws or regulations, such as New York's information security breach and notification law (General Business Law Section 899-aa)
- The event has a reasonable likelihood of materially harming any material part of the Covered Entity's normal operations (23 NYCRR 500.17(a)(2)).

To further assist Covered Entities with their reporting requirements, DFS has **announced a new online portal** to securely transmit Notices of Exemption, Certifications of Compliance and Notices of Cybersecurity Events, as required by 23 NYCRR Part 500.

In anticipation of the August 28, 2017, deadline, Covered Entities should be prepared to implement additional measures, including designating a Chief Information Security Officer (CISO); ensuring qualified Cybersecurity Personnel are in place; establishing a Board-approved written Incident Response Plan and Cybersecurity policies, and implementing infrastructure to limit access to nonpublic information.

Another common misconception is that Covered Entities qualifying for an exception need not comply with the Regulation. According to the FAQs, the exemptions listed in 23 NYCRR Part 500.19 are limited in scope. While certain organizations may be exempt from appointing a CISO, performing penetration testing and maintaining audit trails, they still must comply with the sections listed in the exemptions that apply to covered entities.

These requirements include establishing cybersecurity programs and policies, maintaining record retention and destruction programs, conducting risk assessments, and implementing policies and procedures to ensure the security of nonpublic information maintained by third-party service providers. These programs and policies and the Risk Assessment also must evaluate and address the risks to an information system or its stored nonpublic information presented by a Covered Entity's subsidiary or affiliate.

Colorado

Following in the footsteps of DFS, the Colorado Division of Securities has adopted cybersecurity regulations applicable to broker-dealers, investment advisers and other fund managers who purchase securities or conduct business in the state.

Colorado's regulations are more limited in scope than New York's and implementation is less costly. For instance, they apply only to broker-dealers purchasing securities in the state and investment advisors doing business there. There are no requirements for third-party vendors, and the requirement that broker-

dealers and investment advisors establish written procedures “reasonably” designed to protect “Confidential Personal Information” does not cover publicly available information.

While the Colorado Division of Securities may consider a variety of factors in determining what is “reasonable,” the cybersecurity procedures must include all of the following:

- An annual risk assessment that does not need to be conducted by an independent third party
- Secure email, including encryption and digital signatures for emails containing Confidential Personal Information
- Authentication of clients’ email instructions and employee access to electronic communication
- Disclosure to clients of the risks of using electronic communications.

The Colorado regulations’ most notable contrast from that of the DFS is the lack of a breach notification requirement, which was included in the initially proposed rules. However, entities may still have such obligations as provided by the SEC if they are subject to federal financial regulation and oversight.

Source URL: https://www.natlawreview.com/article/developments-new-york-and-colorado-cybersecurity-regulations