Robinson+Cole

Data Privacy + Cybersecurity

Financial Services Cyber-Compliance

February 2018

New York's Landmark Cybersecurity Regulation Amendment Proposed, Deadlines Looming

On February 15, 2018, banks, insurance companies, and other financial services institutions and licensees regulated by the New York Department of Financial Services (DFS) will be required to file their first certification of compliance with DFS' far reaching cybersecurity regulation (23 NYCRR Part 500) (the Regulation). The Regulation, which became effective on March 1, 2017, is touted as being the first cybersecurity regulation in the nation, requiring significant operational, technology, and reporting changes in order for entities covered by the Regulation (Covered Entities) to comply. By no later than February 15, Covered Entities will be required to electronically file a certification statement through the DFS cybersecurity portal confirming the company's cybersecurity program met the Regulation's requirements for the prior calendar year.

In a press release reminding Covered Entities of the February 15 deadline, DFS Superintendent Maria T. Vullo announced DFS would be incorporating cybersecurity into all DFS examinations and would be adding questions related to cybersecurity to "first day letters," sent by DFS to commence examinations.

As a reminder, the Regulation requires Covered Entities to complete certain tasks for compliance, including, but not limited to the following:

- Cybersecurity Program Covered Entities must implement a cybersecurity program and adopt written cybersecurity policies and procedures. The policies and procedures must be approved by the board or senior management, and be tailored to the specific entity's business model and risk profile.
- Chief Information Security Officer Covered Entities must designate a qualified Chief Information Security Officer and retain cybersecurity personnel who are familiar with the latest cyber threats and countermeasures.
- Periodic User Access Assessments Covered Entities must periodically review employee accessibility to confidential data and computer networks and place appropriate limitations on such access.
- Breach Incidents Covered Entities are required to report to the DFS within 72 hours any "cybersecurity event" when either (i) there is a pre-existing duty to notify a separate government body or regulatory agency of a cybersecurity event (such as, for example, a duty to report to state regulators under New York data breach notification laws), or (ii) the cybersecurity event at issue has a reasonable likelihood of materially harming any part of its normal operations. Covered Entities are required to report even unsuccessful cybersecurity attacks when such attacks are "sufficiently serious to raise a concern."

In addition to the upcoming deadline on February 15, additional requirements under the Regulation will become mandatory over the next two years, including mandates with regard to adopting specific

technological solutions for cybersecurity, such as two-factor authentication. Relevant dates include:

- March 1, 2018: With the one-year transitional period ending, Covered Entities must implement multi-factor authentication, perform regular penetration testing and risk assessments, and offer mandatory cybersecurity training for staff.
- September 3, 2018: With the eighteen-month transition period ending, Covered Entities must encrypt confidential data transmitted over external networks and at rest, monitor user activity, implement secure data disposal procedures, and maintain audit trails of network activity and significant transactions.
- March 1, 2019: With the two-year transitional period ending, Covered Entities must adopt comprehensive cybersecurity risk management programs for third party service providers.

In subsequent Alerts, we will drill down on the requirements under the upcoming deadlines with additional information about DFS' requirements for compliance.

If you or your business have any questions about compliance with the DFS Regulation, please contact Robinson+Cole's Financial Services Cyber-Compliance Team (the CyFi Team).

Linn Foster Freedman | Benjamin C. Jensen | Norman H. Roos

Scott N. Siedor | Carrie C. Turner

For insights on legal issues affecting various industries, please visit our Thought Leadership page and subscribe to any of our newsletters or blogs.