Patterson Belknap

The New York Department of Financial Services Issues Its Final Cybersecurity Regulation

On February 16, 2017, the New York Department of Financial Services ("DFS") issued the final version of its cybersecurity regulation. The regulation, which has seen several iterations since it was first proposed in September 2016, is detailed, far-reaching, and—in some respects—unprecedented. New York Governor Andrew Cuomo has called the new rules a "first-in-the-nation regulation" designed to protect financial institutions and their consumers from cybercrime. For the financial institutions and insurance companies affected, the regulation's scope and requirements will require a fresh and in-depth look at their overall cybersecurity planning, preparedness, governance, and defenses.

Over the last few months, the rules have undergone multiple revisions. The DFS, however, has settled on the final version. And the turn-around time for covered institutions to comply with the final regulation will be quick: the regulation has an effective date of March 1, 2017. Prompt implementation is critical, but companies need to proceed in a manner that is methodical, precise, and appropriately documents the decision-making process at each critical step of the process.

The regulation is detailed and its scope is expansive, but its requirements can be broken down into five, core categories.

Corporate Governance: The DFS regulation requires engagement at the top of an organization. The regulation provides that senior management and boards of directors "must take" cybersecurity issues "seriously and be responsible for an organization's cybersecurity program." This obligation starts with the creation of a cybersecurity policy—the framework for protecting a company's information systems and most sensitive information. Covered companies must also designate a Chief Information Security Officer ("CISO"), who must report to the board annually. The cybersecurity policy must be in place, and the CISO designated, by August 28, 2017.

Testing and Assessments: The regulation requires companies to conduct a number of cybersecurity tests and analyses. First and foremost, companies will have to perform a "risk assessment." The risk assessment must "evaluate and categorize risks," evaluate the integrity and confidentiality of the company's information systems and non-public information, and develop a process to mitigate any identified risks. Companies must also conduct annual penetration testing and bi-annual vulnerability testing. Each of these tests and assessments must be conducted by March 1, 2018.

Day-to-Day Requirements: The regulation's day-to-day and technical requirements are substantial. Among others, companies must develop access controls for their information systems, ensure the physical security of computer systems, encrypt or protect personally identifiable information, perform reviews of in-house and externally created applications, train employees, and build an audit trail system. The timeline to ensure compliance with these rules ranges from one year to eighteen months.

Third-Party Rules: The new regulation not only contains extensive requirements for covered entities, but also regulates third-party vendors with access to an institution's IT network or non-public information. Covered banks and insurers are required to develop and implement written policies and procedures to ensure the security of IT systems or non-public information that can be accessed by their vendors. At a minimum, these policies must identify the risks from third-party access, impose minimum cybersecurity practices for vendors, and create a due-diligence process for evaluating those vendors. Covered entities will have two years to satisfy these extensive requirements.

Notification Requirements: Finally, the new regulation includes a mandatory notification process for any material cybersecurity event. Within 72 hours, companies must report to the DFS a cybersecurity event that has a "reasonable likelihood" of "materially harming" the company or that must be reported to another government or self-regulating agency. In addition, companies—through a certification from either the board or a senior officer—must annually attest to their compliance with the DFS regulation.

Not every DFS-regulated institution will be subject to all aspects of the DFS cybersecurity regulation. The following types of entities can expect some relief from the regulation's strict requirements.

- Companies that earn less than $5 million in gross revenue in New York (in each of the past three years), that have less than $10 million in year-end total assets from all operations, or that have fewer than ten employees in New York (including independent contractors) are exempt from a number of the regulation's provisions.
- Companies that do not have information systems and access to nonpublic information are, likewise, exempt from a number of the DFS requirements.
- Captive insurance companies—both pure and group captive insurers—are also exempt from many of the DFS requirements.
- And, subject to certain limitations, the regulation exempts a small number of entities from the regulation, including Rule 125 certified and accredited reinsurers.

This Alert is a brief summary of key provisions of the final DFS regulation. In the coming weeks, we will publish an implementation guide that covers, in more depth, the nuts and bolts of compliance. If you would like a copy, please contact DataSecurityLaw@pbwt.com.

Craig A. Newman 212-336-2330 cnewman@pbwt.com

Alejandro H. Cruz 212-336-7613 acruz@pbwt.com

Kade N. Olsen 212-336-2493 kolsen@pbwt.com