Patterson Belknap

NYS Cyber Crack Down Looms: What Every Financial Institution, Insurer and Their Board Must Know

With the public comment period closing in a few days, the New York Department of Financial Services (DFS) "first in the nation" cybersecurity regulation is one step closer to becoming law. The regulation – which covers a broad swath of the world's financial and insurance communities by virtue of DFS's presence in the epicenter of the financial world – mandates a broad array of powerful and detailed requirements that far exceed existing federal and state cyber regulation. Indeed, the regulation contains unprecedented requirements, such as board "review" of a required 14-point comprehensive cybersecurity policy and the written certification by a senior corporate officer verifying compliance with the regulation.

The DFS regulation covers more than 3,000 financial institutions and insurers – including foreign and non-New York based entities – that operate by virtue of New York banking, insurance or financial services laws.

Because the regulation goes into effect on January 1st, 2017, covered institutions are scrambling to get their houses in order to comply with the sweeping requirements. And with good reason - the cost of non-compliance with the regulation is steep. DFS not only has the authority to revoke state banking and insurance licenses – obviously an unacceptable result for local and global institutions with a New York presence – but can also pursue enforcement actions against companies and their officers and directors.

In this alert, we detail the key elements of the regulation. We will continue to report on all developments that affect the regulation, including public comments that are filed with DFS and any resulting modifications to the regulation, on our Data Security Law Blog located at http://datasecuritylaw.com.

Background. Late last year, the DFS announced its intention to issue cybersecurity rules to cover financial institutions and insurers that operated under New York law. That announcement came after the DFS surveyed nearly 200 banking and insurance institutions and issued three reports to help inform the rulemaking process. The regulation also comes on the heels of similar rules – by federal regulators.

Which institutions are affected? The DFS regulation covers any entity "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law."

What are the Key Provisions? The proposed cybersecurity regulation is substantial in both its scope and requirements. For example, the proposed regulation includes the following requirements:

- *Cybersecurity Programs*: The program must "identify internal and external cybersecurity threats," use "defensive infrastructure," and detect and respond to cybersecurity events.

- *Cybersecurity Policy*: The policy must address, among other issues, "information security," "business continuity and disaster recover planning," and "vendor and third-party service provider management." The policy must be "reviewed" by the institution's board of directors. A senior corporate officer must certify annually to compliance with the policy.

- *Chief Information Security Officer*: Each institution must designate a "Chief Information Security Officer" to oversee and enforce the cybersecurity program and policy. That officer must issue, at least bi-annually, a cybersecurity report to the institution's board of directors.

- *Testing and Assessments*: Institutions must conduct penetration testing annually and vulnerability testing quarterly.

- *Audit Trails*: Institutions must also "track and maintain data" in order to reconstruct all financial transactions in the event of a breach, to log all electronic access of critical systems, and to monitor alterations made to an audit trail. This information must be maintained for at least six years.

- *Risk Assessment*: Annual risk assessment must also be conducted of an institution's information systems.

- *Limited Access Privileges*: There must also be a periodic review of access privileges to the firm's information systems and restrictions on access to only those persons with a legitimate need.

- *Multi-Factor Authentication:* Firms are also required to use two different types of authentication factors – such as a token, password or biometric measurement – for access to internal systems from an outside network and for access to nonpublic information.

- *Encryption*: Subject to a phase-in period, firms are required to encrypt nonpublic information that they hold and transmit.

- *Cybersecurity Personnel*: Covered entities must "employ cybersecurity personnel" to manage cyber risks and perform core functions.

And there are a number of other proposed rules ranging from training to monitoring obligations.

Third-Party Relationships. Firms must implement policies to ensure the security of information systems and private information accessible by third-party vendors. In the first instance, firms must identify any risk posed by their vendors and review—at least annually—the adequacy of vendors' cybersecurity practices. The regulation also requires covered entities to "include[] in contracts" with third parties provisions requiring multi-factor authentication, proper encryption, and prompt notice in the event of a breach. And a contracting third party must agree to provide "identity protection services" in the event of a breach from that third party's "negligence or willful misconduct."

Reporting Requirements. The regulation also includes *mandatory* reporting requirements. In the event of a data breach, the institution must notify DFS within 72-hours. Firms must also inform the DFS of any cybersecurity event that "has a reasonable likelihood" of impacting the entity's "normal operation" or any nonpublic information. Companies must also "maintain for examination . . . all records, scheduling and data supporting…."

Should you have any questions, please contact:

Michael F. Buchanan 212-336-2350 mfbuchanan@pbwt.com

Michelle W. Cohen 212-336-2758 mcohen@pbwt.com

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