BRACEWELL

INSIGHTS

New York DFS Finalized Cybersecurity Regulations Go Into Effect March 1, 2017

March 1, 2017

On February 16, 2017, the New York State Department of Financial Services (DFS) announced the final version of the "first-of-its-kind" cybersecurity regulations governing financial institutions, insurance companies, and other DFS-regulated entities. The regulations will become effective March 1, 2017, with a staggered implementation period to comply with key requirements. While the regulations largely contain many prudent practices that covered firms may already have in place, given the tight timeline for implementation, firms would be wise to assess their existing cybersecurity measures for compliance with the new requirements.

In the regulations, DFS imposes certain minimum standards rather than only specific requirements, a tacit acknowledgment that the regulations cannot be so overly prescriptive or "one-size fits all" that firms are unable reasonably to adapt their programs to technological advances. The regulations are designed to both protect the nonpublic information of individual consumers and the integrity of the state's financial services industry more broadly. Initially released in September 2016, with final regulations expected to be effective on January 1, 2017, DFS issued a new draft of the proposed rules in late December which incorporated industry comments, followed by an additional public comment period.[1]

The final regulations require, among other things:

- Corporate governance controls, including the appointment of a chief information security officer who will be responsible for reporting annually to the entity's board of directors or equivalent body;
- Assessments of risk and the design of policies and procedures tailored to an entity's needs, including, but not limited to, access controls and identity management; business continuity and disaster recovery planning and resources; incident response planning, and data governance and classification;
- Reporting to DFS within 72 hours of any cybersecurity event that has a "reasonable likelihood of materially harming any material part" of an entity's operations;
- Documentation of identified material deficiencies, remediation plans, and annual certification of compliance with the regulations; and
- Supervision of and requirements relating to third-party service providers.

Notably, DFS states in the regulations that senior management must "take [the cybersecurity] issue seriously and be responsible" for the cybersecurity program. The requirement that a board of directors or senior officer certify a firm's compliance with the regulations each year indicates that DFS will be scrutinizing firms for compliance from the C-suite down. This requirement echoes similar DFS certification obligations, namely, in its anti-money laundering regulations, which went into effect January 1, 2017. It remains to be seen how aggressively DFS will enforce the various certification provisions, but the regulator has clearly signaled its intention to hold senior management to account.

The supervision of third parties is another significant area for covered entities. Regulators are closely scrutinizing the use and supervision of third parties that handle customers' personal information,[2] and DFS will be no exception. The DFS regulations require firms to (i) identify the risks arising from third-party access to IT systems and nonpublic information, (ii) require third-party adherence to cybersecurity practices, and (iii) create a due-diligence process for vetting vendors on an initial and periodic basis.

Firms have a six-month grace period to comply with certain of the regulations, with longer transition periods for some provisions as follows:

- By March 1, 2018, firms must comply with CISO reporting requirements and implement penetration testing and vulnerability assessments, risk assessment, multi-factor authentication, and cybersecurity awareness training;
- By September 1, 2018, firms must comply with requirements relating to audit trails, application security, data retention, monitoring procedures, and encryption of nonpublic information;
- By March 1, 2019, third-party service provider security policies must be implemented.

In sum, while DFS may be the first state regulator to impose mandatory cybersecurity regulations on financial institutions, firms may already have effective measures in place, as required by federal banking regulators. It is critical, however, to review existing policies and procedures to ensure that they comport with DFS expectations and that they have been implemented effectively. Enforcement of the new regulations is likely to be a high-profile priority for DFS, and a proactive approach is best for covered entities going forward.

The DFS regulations, proposed 23 N.Y.C.R.R. Part 500, are available ***here***.

---

[1] See Bracewell's past commentary on the proposed regulations ***here***.

[2] See, for example, Bracewell commentary on a FINRA enforcement brought against Lincoln Financial Group ***here***.