January 10, 2017

Responding to Pushback, New York Regulators Revise Proposed Cybersecurity Regulations

Last fall, with some fanfare, the New York State Department of Financial Services (DFS) announced proposed cybersecurity regulations. As we previously reported, in a break from prior, high-level standards, the proposed regulations shifted toward a more prescriptive approach, mandating specific policies, onerous government notification requirements, and hands-on oversight from corporate leaders. Commentators and financial industry groups pushed back during the comment period. In response, on December 28, 2016, DFS released revised regulations, which, subject to further comment, will now become effective on March 1, 2017.

While the revised regulations remain demanding, they do ease some of the original proposed requirements and restore a degree of deference to management, particularly in regard to risk assessment and mitigation. Compared to the original proposal, the amended regulations:

- Narrow the previously expansive definition of individuals' nonpublic information that must be protected.

- Link the cybersecurity requirements to institutional risk, permitting required policies, including penetration testing and audit systems, to be based on, or developed in accordance with, an institution's own internal risk assessments.

- Lessen the frequency of some of the new monitoring, testing, and reporting requirements, including those related to vulnerability and security assessments.

- Reduce the new government notification requirements, limiting required reporting to events that materially harm operations or must be reported to other government agencies. The revisions maintain a 72-hour reporting time frame, but permit the clock to start ticking only when an institution has determined that a triggering event has occurred.

- Ease corporate leadership oversight requirements, at least to some extent. But covered institutions must still be cognizant of the significant new requirements that remain, including board or senior officer approval of cybersecurity policy, board review of annual written CISO reports, and annual compliance certifications by board chairs or senior officers, with false certifications carrying potential civil and criminal penalties.

We see the revised regulations as an improvement over the initial proposal. Still, they represent a significant departure from the *status quo*, heralding a more active role for regulators in setting private sector cybersecurity standards. With federal financial regulators preparing to issue cybersecurity rules in 2017, it remains to be seen whether DFS's revised approach will prove to be an outlier or a harbinger of a new regulatory approach to cybersecurity.

John F. Savarese
David M. Silk
Wayne M. Carlin
Sabastian V. Niles
Marshall L. Miller
Jorge M. Gutierrez, Jr.