LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

September 2016

Breaking News:

Much Ado About 'Minimum Standards' for DFS Cybersecurity Regulation

By Chris Stecher and Justin Hectus

The New York State Department of Financial Services (DFS) made headlines on September 13 by announcing a "first-in-the-nation," comprehensive cybersecurity regulation, which will mandate 16 "minimum standards" for the 4,000+ institutions operating under DFS jurisdiction. From a practical perspective, the proposed regulation adopts or aligns with guidance from the 2014 National Institute of Standards and Technology (NIST) Framework, portions of the Fair Trade Commission's 2015 Start with Security program, as well as the basic requirements that banks have established and enforced for their third party vendors for several years. In short, there is nothing revolutionary or innovative in the proposed regulation. Indeed, the DFS acknowledges that "many firms have proactively increased their cybersecurity programs with great success," and its own 2013 survey found that 90% of institutions (and 98% of large institutions) had implemented a comprehensive information security framework. Notwithstanding sensational headlines, a review of the volume of significant breaches at financial institutions over the last decade supports the conclusion that financial institutions are taking cybersecurity extremely seriously; large data breaches occur less and less frequently, and the root cause seldom is poor security. All of this begs the questions — why the need for New York's proposed regulation, and what will be the practical impact for financial and other institutions across the country?

Chris Stecher is a Shareholder with Keesal, Young & Logan's San Francisco Office. Chris litigates employment and securities cases in arbitration and courts throughout the United States. He also regularly advises clients in areas such as employee discipline, employee and customer privacy laws, trade secret issues, and compliance with other local, state and federal laws. Chris is admitted to practice law in California and Washington. **Justin Hectus** is the Director of Information at Keesal, Young & Logan where he oversees a variety of operational functions including the direction of the firm's IT vision, strategy and execution. A member of this newsletter's Board of Editors and a two-time ILTA Distinguished Peer Award winner, Justin and KYL have established a decades-long track record of effectively leveraging leading edge technology to achieve outstanding results on behalf of the firm's clients.

The Devil is in the Details

At first blush, the proposed regulation appears very onerous. However, the proposed minimum requirements fit squarely under the umbrella of minimum standards for the most part. Many Chief Information Security Officers (CISOs) at medium and large institutions will read the 16-point list and say, "check, check, check, check …," shrug their shoulders, and move on. The two likely exceptions will be aspects of the notice requirement and another aspect of the training requirement. Regarding notice, the proposed regulation will require covered entities to notify New York's Superintendent of Financial Services of any cybersecurity event that has a "reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information" within 72 hours of becoming aware of the event. Although providing prompt notice of actual cybersecurity breaches seems to make sense, mandating that notice for events involving the "potential unauthorized tampering with, or access to or use of, Nonpublic Information" appears overly broad, and many financial institutions may object to the fuzzy, subjective wording of the regulation. Hopefully, standards will be clarified during the comment period. On the training front, requiring "all personnel to attend regular cybersecurity awareness sessions" will present a challenge for some institutions.

On a smaller scale, the very limited exceptions defining which entities are exempt from the regulation (1,000 customers *and* less than $5M gross annual revenue *and* less than $10M in assets) will thrust many small businesses into the uncomfortable position of rapidly deploying people, policies and technology to come into compliance. Particularly challenging will be designating a "qualified individual" to serve as CISO or to oversee

a third party serving in that role. There remains a shortage of qualified cybersecurity professionals at every level and particularly at the most senior levels. Smaller institutions with less defined structures may have to rely on vendors, such as Software as a Service, Security as a Service and now "CISO as a service" in order to meet the new requirements.

Business Implications

Incremental improvement in cybersecurity has been the theme for years at medium and large regulated institutions and the medium and large service providers (including law firms) that serve the financial industry. For smaller regulated institutions and smaller third-party service providers, however, the proposed regulation will present some real difficulty if enacted as proposed. Many small regulated businesses do not even have the expertise to properly assess their current cybersecurity capabilities, let alone to come into compliance with the proposed regulation in the 180 days allowed. The trickle-down effect of the requirement that third-party service providers are assessed "at least annually" and that they meet the same standards outlined in the proposed regulation will also likely encourage vendor consolidation and will leave some small vendors out in the cold. The DFS' 2014 survey regarding Third-Party Service Providers indicated that "some banking organizations have exemptions from their customary due diligence for individual consultants and professional service providers (*e.g.*, legal counsel)." It seems unlikely that those exceptions will be allowed in the future if the proposed regulation is adopted in its present form.

Given the shortage of qualified cybersecurity professionals and the potential volume of real and potential cybersecurity events, DFS investigations and enforcement may present significant challenges and potential new liability. One potential scenario could be that the DFS levies fines post-breach. Once the DFS confirms that data has been compromised, it could determine with the benefit of hindsight whether a covered entity was in compliance with the regulation prior to the breach and assess penalties retroactively.

The regulation will likely be a boon for cyber-experienced professional service firms that can serve in an audit or advisory capacity for the industry. Likewise, there is a business opportunity for new one-stop-shop vendors to provide outsourced compliance for smaller entities. As discussed in an article published in the September issue of *Cybersecurity Law and Strategy* and *Inside Counsel*, outsourcing and technology as a service provide solutions that scale to even one person shops, offering sophisticated security without the overhead of infrastructure.

The Wrong Conversation?

Some of the commentary related to the proposed regulation has rightfully focused on the burden and additional costs, as well as the potential risk that minimum standards will actually discourage innovation and exceptional efforts in cybersecurity. There certainly is some merit to those concerns. However, given the increasing reliance on technology for all of our everyday tasks and the increased public and regulatory scrutiny of cybersecurity, New York's proposed regulation soon may very well be the rule, as opposed to the exception. If and when that happens, entities (in both the financial services industry and any industry that uses a computer) that have adopted the minimum standards listed in the proposed regulation will be better equipped to defend against cyberattacks and other security breaches that are rapidly increasing in volume, complexity and impact. From a practical perspective, these minimum standards line up with baseline expectations that have been the standard for years. Moreover, entities that are have been investing in improving their cybersecurity systems likely will reap the benefit of, among other things: 1) decreased costs in the long run as the world moves closer to a paperless reality; 2) improved defenses if and when regulatory inquiries or lawsuits related to security breaches arise; and 3) improved protection of company and customer confidential information.

The conversation, therefore, might be better shifted toward the progressive end of the spectrum. In the 90's, similar conversations took place surrounding technology and efficiency gains, suggesting that there was competitive advantage to investing in people, process and technology. What was previously viewed as a cost center was repackaged as a "differentiator" where businesses and consumers alike were the beneficiaries. Cybersecurity is still viewed by many as the cost center of our day when it should be a differentiator leveraged for competitive advantage and for the benefit of our current and prospective clients, as well as our overall business.

New York's proposed regulation could implicate federal pre-emption, separation of power and perhaps many other legal issues that may take years to play out in the courts. However, those companies that match innovative technology solutions with an exceptional cybersecurity defense posture will be positioned to survive and, in fact, thrive in this critically important area.

Important Dates

A 45-day public comment period open Sept. 28, 2016 for the proposed regulation, which is slated to become effective on Jan. 1, 2017 after which covered entities will have 180 days to comply.

—❖—