New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 40
MONDAY, AUGUST 28, 2017

Outside Counsel

Expert Analysis

Grace Period Expires for Cybersecurity Regulations in NY: What Comes Next?

By **F. Paul Greene**

The day has finally arrived for the financial services industry in New York. The new cybersecurity regulations issued by the New York State Department of Financial Services are officially in force, after a 180-day grace period that followed the effective date of the regulations, March 1, 2017. These regulations, found at 23 N.Y.C.R.R. Part 500, mark a watershed moment in cybersecurity regulation in the United States. For the first time, a single state is regulating cybersecurity on a potentially global scale, and it has done so via the regulatory process, not legislative action.

These two developments change the landscape of cybersecurity regulation in two very distinct ways. *First*, by focusing on a global industry regulated within the state, Part 500 magnifies the potential reach of a state regulatory body immensely. Part 500 impacts not only covered financial institutions (defined as Covered Entities), but also third parties located around the world that provide services to these institutions. This is because of the defined Third Party Service Provider Security Policy required by Part 500, under which a Covered Entity must set certain "minimum cybersecurity practices" for every third party service provider doing business with the Covered Entity. It is perhaps because of this potential global reach that DFS attached a two-year phase-in period to the Third Party Service Provider Security Policy requirement.

> Regardless of what comes next, one thing is guaranteed with Part 500: The new "normal" in cybersecurity regulation is that there is no static state of normalcy.

Second, by choosing the regulatory process to implement Part 500, New York has doubled down on the trend in cybersecurity regulation to infer broad regulatory authority from very general enabling statutes. Case in point, the Federal Trade Commission's extensive efforts to regulate cybersecurity based solely on the general language of the Federal Trade Commission Act. In relation to DFS, the enabling statutes referenced in Part 500 are as silent on cybersecurity as their FTC counterparts. They concern, rather, the department's authority to regulate the financial services industry in New York generally, including its ability to issue fines.

By steering clear of the legislative process and the gridlock that can often accompany it, DFS has paved the way to dramatically accelerate the pace of change in cybersecurity regulation. By its very nature, the

F. PAUL GREENE *is a partner and chair of the privacy and data security practice group at Harter Secrest & Emery. He can be reached at fgreene@hselaw.com.*

regulatory process is more nimble and less deliberative than the legislative process. In New York, a new or amended regulation can be put in place after a 45-day notice-and-comment period. Compare that to the New York state legislature, which has been considering changes to the state's data breach notification law, New York General Business Law §899-aa, for several years already. Add to that the ability of an administrative agency in New York to issue emergency regulations without any prior notice at all, and repeatedly re-promulgate those emergency regulations for additional 60-day periods, and the pace of potential change increases exponentially.

These developments have not gone unnoticed, with at least one other state, Colorado, issuing cybersecurity regulations for the financial sector. If history is any guide, we can expect to see proliferation of state cybersecurity regulations, instead of legislation, not only in the financial sector, but also in other areas of concern to states, for example critical infrastructure, education, health care, or employment law.

Guidance

Another key component of the regulatory process is the role of agency guidance. Beginning in April of this year, DFS began issuing FAQs in relation to Part 500, addressing potential ambiguities in the regulations. This kind of regulatory guidance helps fill some of the interpretive gaps that can arise in a complex set of regulations. But such "guidance" can simultaneously add to the complexity of compliance, with the agency placing a gloss on the regulatory language that may conflict with its literal requirements.

For example, DFS's most recent Part 500 FAQ addressed the controversial 72-hour reporting window for certain defined Cybersecurity Events. Under this requirement, Covered Entities must report a Cybersecurity Event to DFS within 72 hours of a determination that the Event has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." See 23 N.Y.C.R.R. §500.17(a)(2). As defined in Part 500, a "Cybersecurity Event" can include an unsuccessful attempt to "gain unauthorized access to, disrupt or misuse" a Covered Entity's information system or data stored on that information system.

Hence, an unsuccessful phishing attempt directed at harvesting system credentials or an unsuccessful ransomware attack could each be reportable. The problem is that these kinds of attacks are often automated, and can occur frequently, coupling low probability of success with high potential harm.

Addressing this issue, DFS pointed to the requirement under Part 500 that a Covered Entity conduct a defined Risk Assessment when creating a Part 500 compliance program. As in other cybersecurity regulatory schemes such as HIPAA and the Gramm-Leach-Bliley Act, the Part 500 Risk Assessment is the cornerstone upon which a security team can base its security compliance decisions. Further, according to DFS, when deciding on whether an unsuccessful Cybersecurity Event is reportable, a Covered Entity can rely on its "good faith judgment" and its Part 500 Risk Assessment in determining whether the four-part test of §500.17(a)(2) has been met. DFS went on to note that "[t]he Department anticipates that most unsuccessful attacks will *not* be reportable … ." See Frequently Asked Questions Regarding 23 NYCRR Part 500, available at www.dfs.ny.gov/about/cybersecurity_faqs.htm.

These three qualifiers—good faith judgment, reliance on Risk Assessment, and that the majority of unsuccessful attacks will not be reportable—do not appear in §500.17(a)(2), although a Covered Entity could have argued that they were certainly implied by the spirit and language of Part 500 generally. The FAQs, however, remove uncertainty in this regard, allowing Covered Entities concrete guidance on how the new regulations will be interpreted in practice.

This flexibility inherent in regulatory guidance can extend both ways, however, creating new requirements in the gaps between regulatory sections, as inferred or interpreted by the administrative agency. Hence, a Covered Entity must not only keep its eye on the State Register for any amendments to Part 500, it must regularly review the DFS FAQs page for relevant guidance. Since April 2017, when the FAQs first appeared, DFS has added to or edited them at least once.

And the DFS FAQs page was where DFS announced its secure reporting portal for Part 500-related submissions. A Covered Entity that did not know of the FAQs page would have missed the portal announcement. No statewide mailing or notice in the State Register was made or given in relation to the portal, further underscoring the importance of the FAQs page.

With the 180-day grace period for compliance with Part 500 expiring today, the question follows as to what comes next. As an initial matter, DFS will have to receive, review and react to the numerous notices of limited exemption that are due as of Sept. 27, 2017 for Covered Entities that have determined that they qualify for a limited exemption to Part 500, because, for example, they have fewer than 10 employees or less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations.

The remainder of Covered Entities have until Feb. 15, 2018 to submit a certification of compliance with Part 500 for the prior calendar year, ostensibly Aug. 28, 2017 to December 31, 2017. At that point, DFS will again need to receive, review, and react to a large number of filings, numbering in the thousands. Certainly, given the broad scope of Part 500, it is likely that organizations that are not Covered Entities will mistakenly certify that they are, and other organizations that are Covered Entities will mistakenly conclude that they are not.

Like the ever-changing threats organizations face to their information systems, cybersecurity regulation will remain in flux, requiring vigilance, flexibility, and resilience as organizations create and calibrate compliance programs accordingly.

These administrative issues will likely command much of DFS's attention in the first few months of Part 500 implementation. Further, depending on the level of reporting that occurs, DFS may become inundated with Cybersecurity Event reports flowing in through its secure portal. And of course it remains to be seen what DFS will do with the information it receives. Section 500.18 of the new regulations potentially exempts information provided to DFS under Part 500 from FOIL disclosure, but that does not mean that DFS will not report generally on number and types of attacks reported, or that the legislature will not override the regulations and require that reporting to DFS on Cybersecurity Events be made public, in whole or in part. Indeed, precedent for this kind of public breach reporting exists just across New York's eastern border, with the Massachusetts legislature recently making public the information gathered in its breach reporting archive, which includes name of the breached entity, the records involved (e.g., driver's license number, SSN), and whether or not the records were encrypted.

Regardless of what comes next, one thing is guaranteed with Part 500: The new "normal" in cybersecurity regulation is that there is no static state of normalcy. Like the ever-changing threats organizations face to their information systems, cybersecurity regulation will remain in flux, requiring vigilance, flexibility, and resilience as organizations create and calibrate compliance programs accordingly.

Reprinted with permission from the August 28, 2017 edition of the NEW YORK LAW JOURNAL © 2017 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-08-17-45