New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 39
WEDNESDAY, MARCH 1, 2017

Outside Counsel

Expert Analysis

Final DFS Cybersecurity Regulations: Questions of Scope and Effect Linger

By **F. Paul Greene**

It has been a wild ride for the banking, insurance, and financial services industries in New York over the past five months. Last September, the New York State Department of Financial Services (DFS) proposed sweeping new cybersecurity regulations for these industries. The proposed regulations were heavily prescriptive, requiring certain specific security controls regardless of circumstance, and drastically altering the regulatory landscape for thousands of companies governed by DFS.

DFS received over 150 separate comments to the proposed regulations, many of which criticized their sweeping scope and prescriptive nature. In response, DFS made significant revisions, publishing a notice of revised rulemaking on Dec. 28, 2016. These revisions marked a shift from a prescriptive approach to a more risk-adjusted approach, which is more in line with the regulatory frameworks that many DFS regulated-entities are already subject to, such as the Gramm-Leach-Bliley Safeguards Rule and HIPAA.

> The new DFS regulations are certainly not the end of the story, when it comes to cybersecurity regulation in New York.

On Feb. 16, 2017, DFS released the final version of its new regulations, making further incremental changes, but maintaining its new risk-adjusted approach, requiring a periodic defined Risk Assessment to determine applicability of certain security controls, such as multi-factor authentication and encryption. Important questions concerning the scope and effect of the regulations remain, however.

'Minimum' Standards, or Not?

The originally proposed regulations made 12 separate references to "minimum" standards that a regulated entity (defined as a Covered Entity) should implement. The revised version removed nine of these references, which remains the case in the final version.

The problem with minimum standards, of course, is in determining whether the regulatory "minimum" is ever good enough. Certainly, no Covered Entity wants to publicize that it is doing only the bare regulatory minimum to protect its networks. Similarly, setting a "minimum" standard could cause a Covered Entity to overspend on its cybersecurity efforts, unsure of exactly what standard DFS might find appropriate.

In its revisions, DFS apparently wanted to eliminate this confusion, but ambiguity remains. Two

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.*

of the remaining three references to "minimum" standards appear in the preamble to the proposed regulations, and arguably do not materially alter the risk-adjusted approach that follows. The third reference is in proposed §500.11, entitled "Third Party Service Provider Security Policy." Under this section, a Covered Entity is required to develop and maintain a cybersecurity policy concerning third parties with access to the Covered Entity's systems or protected information. Subject to the Covered Entity's Risk Assessment, this policy must address "minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity." See 23 N.Y.C.R.R. §500.11(a)(2) (final rule). In applying this rule, it will be difficult for Covered Entities to find the right "minimum" level of controls required of their third-party service providers. If the service provider is the weak link in a breach, hindsight can certainly call into question whether a Covered Entity's "minimum" standards were sufficient. Rarely are breached entities seen as blameless, especially when it comes to managing third parties with access to their systems.

It is unclear whether DFS intended to leave these references to "minimum" standards in the final regulations, or whether this is a case of incomplete editing. This question is a familiar one in the legislative and regulatory process. Case in point, the recent amendment to the Tennessee data breach notification statute, Tenn. Code §47-18-2107, which removed an encryption-related safe harbor from the statute's definition of breach, but not from the statute's definition of protected "Personal information." See Tenn. Code §47-18-2107(a)(3)(A). This amendment has caused confusion in the industry as to whether the Tennessee encryption caveat has been removed or not.

Regulations vs. Legislation

The new DFS regulations mark the state's first foray into direct cybersecurity regulation, as compared to addressing cybersecurity via legislation. Up to now, the primary, state-level rule concerning cybersecurity in the private sector in New York was found in N.Y. Gen. Bus. Law §899-aa, the New York data breach notification statute. As is the case with the 46 other state-level data breach notification statutes, §899-aa had a collateral effect on cybersecurity practices, with companies hardening their controls so as to avoid a data breach in the first place, thereby avoiding the necessity of state-mandated breach notification.

Section 899-aa is a statute, however, and took nearly two years to pass. The new DFS regulations, by contrast, were finalized in less than five months, with a combined 75 days of comment period for interested parties to submit input or criticism. Further, DFS, not the state legislature, decided whether and to what extent to incorporate comments received concerning the regulations. Lastly, the regulations are to be promulgated under §§102, 201, 202, 301, 302, and 408 of the Financial Services Law. These sections do not specifically concern cybersecurity, but rather govern DFS's general authority to regulate the banking, insurance, and financial services industries, including its ability to issue fines for violation of DFS regulations. From this very general authority, DFS has postulated the ability to issue cybersecurity regulations, an approach that has been upheld on the federal level in relation to the Federal Trade Commission and its efforts to regulate cybersecurity under the auspices of the FTC Act, albeit without specific regulations.

As for timing, DFS can change or add to its new regulations on an emergency basis with immediate effect, if DFS finds that such changes are necessary "for the preservation of the public health, safety or general welfare." See N.Y. State Admin. Proc. Act §202(6)(a). Certainly, one can conceive of a cyber threat significant enough to the financial services industry to warrant, or at least trigger, immediate action from DFS, changing its cybersecurity rules.

Scope of Protected Information

The initially proposed regulations included a definition of

protected Nonpublic Information that encompassed effectively all personally identifiable information (PII) in a Covered Entity's possession not obtained from public sources. This, of course, sent shock waves throughout the industry.

In response, DFS narrowed its focus on PII to correspond generally to the definition of protected "private information" contained in N.Y. Gen. Bus. Law §899-aa, specifically an identifier plus another more sensitive data element, such as Social Security number; driver's license number; or account or payment card number, together with account credentials, such as a security code. DFS added biometric information to this list as well, echoing efforts on the legislative level to add biometric information to the scope of §899-aa.

This appeared to limit the scope of the DFS regulations, but did it? Under the final regulations, Nonpublic Information still includes "[b]usiness related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity." See 23 N.Y.C.R.R. §500.01(g)(1) (final rule). This, of course, would encompass any compromising emails or other unfavorable information on a Covered Entity's network, the unauthorized disclosure of which would have a material adverse effect on a Covered Entity. It would also include all of a company's operational information, which, in the case of a ransomware attack, could become encrypted, rendering it unusable until the ransom is paid. This extends the definition of Nonpublic Information in the regulations far beyond traditional PII, and questions whether the definition has been limited at all, as a practical matter.

Coverage Questions

The initially proposed regulations created confusion among DFS-regulated entities, many of which may not have been aware that they were regulated by DFS, as to the reach and scope of the regulations. Case in point, charitable organizations that issue annuities in New York under §1110 of the Insurance Law. According to the DFS website, there are 377 separate such entities, including 51 separate colleges and 68 universities, from both New York state and around the nation. Based upon commentary DFS received, DFS has excluded these organization from its final rule. That being said, uncertainty still abounds, for example in relation to entities that devote only part of their operations to DFS-regulated activity, but nevertheless maintain an integrated network. The new regulations, as written, do not differentiate between the portions of a Covered Entity's network that pertain to DFS-regulated activities and those that do not, leaving such entities in limbo as to whether DFS controls apply to their entire network, or only a smaller subset. Clarity on this issue will have to come from either DFS guidance, amendment of the regulations, or enforcement precedent.

Stay Tuned

The new DFS regulations are certainly not the end of the story, when it comes to cybersecurity regulation in New York. As cyber threats develop and intensify, regulators and legislators will react, and the rules concerning cybersecurity will change. In this regard, the trend has been toward more regulation, not less. Hence, DFS's "first-in-the-nation" regulations may well become a new cybersecurity floor, rather than a ceiling, both in New York and beyond.