New York Law Journal
Corporate Update
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 60
THURSDAY, MARCH 29, 2018

FINANCIAL SERVICES

NY DFS Issues Sweeping FAQs Affecting Scope of Regulations

By F. Paul Greene

The cybersecurity regulations from the New York State Department of Financial Services (DFS) that went into effect on March 1, 2017 have had wide-reaching effects in the financial services industry and beyond. Their sweeping scope—applying to any person or entity licensed or otherwise operating under an authorization under the New York Banking, Insurance, or Financial Services Laws—brought thousands of entities into the DFS' reach, many of which had had only tangential dealings with DFS in the past.

Case in point: higher education institutions that issue charitable annuities. These institutions are licensed under the New York Insurance law, but for many of them, it came as a surprise that DFS could possibly consider them to be a defined "Covered Entity" under the originally proposed regulations, which were amended and promulgated at 23 N.Y.C.R.R. Part 500. As part of those amendments, and in response to concern from higher education institutions and groups, DFS exempted issuers of charitable annuities from the scope of Part 500. See 23 N.Y.C.R.R. §500.19(f).

Open questions remained for other entities, however, specifically federally chartered banks that function as "exempt mortgage servicers" in New York and certain health care entities, such as Health Maintenance Organizations (HMOs) and Continuing Care Retirement Communities (CCRCs). DFS's primary outlet for regulatory guidance in relation to Part 500 has been its FAQs webpage, available on the DFS website. Since the promulgation of Part 500, DFS has used the FAQs page to clarify certain areas of confusion within the regulations, including as to their scope and reach. With these FAQs, DFS is following the lead of other agencies in the cybersecurity regulatory space, such as the Federal Trade Commission, which regularly provide privacy and cybersecurity guidance via their websites.

On Feb. 21, 2018, DFS issued sweeping new FAQ guidance.

On Feb. 21, 2018, DFS issued sweeping new FAQ guidance. Specifically, DFS stated that exempt mortgage servicers are not Covered Entities under Part 500, unless they were granted an exemption under the Commissioner's discretion addressed in 3 N.Y.C.R.R. Part 418.2(e). (Federally chartered banks are usually exempt from registration as a mortgage servicer in New York State under Banking Law §590, and do not require an exemption under Part 418.2(e).) This was certainly a judgment call by DFS, and a welcome one for federally chartered banks, because under Banking Law §590, exempt mortgage servicers are required to "compl[y] with any regulation applicable to mortgage loan servicers, promulgated by the superintendent," which includes Part 500. See N.Y. Banking Law §590(2-b)(1).

In the same FAQ that exempts federally chartered exempt mortgage servicers from Part 500, however, DFS also "encourage[d] all financial institutions, including exempt Mortgage Servicers, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500." Although non-binding, such administrative "encouragement" carries profound weight, especially with the rise of state legislatures, including in New York, considering and sometimes passing laws requiring "reasonable [cybersecurity] safeguards." In New York, this has taken the form of the SHIELD Act, S. 6933, currently working its way through the budget process. The SHIELD Act would amend New York General Business

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.*

Law §899-aa to add a requirement for "reasonable safeguards to protect the security, confidentiality and integrity of [] private information including, but not limited to, disposal of data." It is not a great leap of logic for a state regulator to conclude that Part 500 has set a baseline of what constitutes "reasonable" cybersecurity safeguards for financial institutions in New York, and perhaps elsewhere, especially in light of DFS's "encouragement" that financial institutions not covered by Part 500 nevertheless voluntarily adopt its safeguards.

Entities not so lucky under the new FAQs include HMOs and CCRCs, which DFS has confirmed are Covered Entities under Part 500. HMOs and CCRCs, however, function primarily in the health care field, and may view their interaction with DFS as secondary to their main operations. In DFS's defense, however, these entities are licensed under the New York Public Health and Insurance Laws respectively, and therefore fit the strict definition of "Covered Entity" under Part 500. In this regard, DFS explained:

> Pursuant to the Public Health Law, HMOs must receive authorization and prior approval of the forms they use and the rates they charge for comprehensive health insurance in New York … . CCRCs are required by Insurance Law Section 1119 to have contracts and rates reviewed and authorized by DFS. The Public Health Law also subjects HMOs and CCRCs to the examination authority of the Department.

Based on DFS's authority to approve forms and rates for these entities, and based upon DFS's examination right (which DFS may have exercised on a limited basis for these entities in the past), DFS asserts in its FAQs that HMOs and CCRCs fall under the purview of Part 500. This is an example of a regulated entity facing sweeping new requirements from its non-primary regulator. The New York State Department of Health, which is the primary regulator for most health care entities in New York, has no cybersecurity regulations for these entities. Rather, at least for HMOs, the federal Department of Health and Human Services has governed (and continues to also govern) their cybersecurity efforts prior to the promulgation of Part 500, specifically under the HIPAA Security Rule, 45 C.F.R. §§164.302-164.318. Now, HMOs, like other health insurance carriers in New York, must answer to two cybersecurity masters: HHS and DFS.

DFS went on in the new FAQs to address the effect that a merger or acquisition might have on a Covered Entity under Part 500. Specifically, DFS stated that a merger or acquisition for a Part 500 Covered Entity brings with it a duty to undergo a factual analysis of how the acquisition may affect the Covered Entity's compliance duties. According to DFS, "important considerations include, but are not limited to, what business the acquired company engages in, the target company's risk for cybersecurity including its availability of PII, the safety and soundness of the Covered Entity, and the integration of data systems." This requirement was arguably already contained in Part 500, specifically in §500.09(a) (Risk Assessment), which requires a Covered Entity to update its Risk Assessment "as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information, or business operations." It is also akin to the requirement under the Gramm-Leach-Bliley Act Safeguards Rule that a Financial Institution "evaluate and adjust [its] information security program in light of … any material changes to [its] operations or business arrangements." See 16 C.F.R. §314.4(e). Hence, this FAQ may come as common sense to many financial institutions, but it is helpful for others that may not have had robust Gramm-Leach-Bliley compliance programs in place in the past.

These new FAQs, and the FAQs issued previously, help clarify areas of uncertainty under Part 500. The problem with the FAQs, however, is that they are non-binding and can be changed at will, however unlikely an abrupt or material change from DFS may be. Specifically, FAQs and other regulatory guidance can serve as a gloss to the letter of the regulation at issue, but they cannot change the regulations themselves, or conclusively bind the administrative agency to a certain interpretation of the regulations in the future. Changes to Part 500 itself can only be made by the 45-day notice and comment rulemaking procedures required under the State Administrative Procedure Act, or—potentially—via 90-day, renewable emergency regulations, which can become effective immediately. Accordingly, both Covered Entities and exempted entities such as issuers of charitable annuities and federally chartered exempt mortgage servicers must remain vigilant to see whether and how the scope of Part 500 will change in the future. This includes watching both the DFS FAQ page for future regulatory guidance, staying abreast of any public statements DFS may make about Part 500, and watching the State Register for future proposed amendments or emergency regulations. If the limited history of Part 500 is any guide, such change is sure to come.