New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 256—NO. 79
MONDAY, OCTOBER 24, 2016

Outside Counsel

Expert Analysis

New Regulations Add to Complexity Of Cybersecurity Compliance

By **F. Paul Greene**

On Sept. 13, 2016, the New York State Department of Financial Services (DFS) published draft regulations addressing cybersecurity in the financial sector. Described as "first in the nation," the draft regulations are sweeping in scope and reach well beyond core financial institutions, such as banks and lenders. A 45-day notice and comment period is under way, ending on Nov. 13, 2016, which will be followed by a summary from DFS of the comments received and DFS's responses to those comments. The new rules then become effective, unless DFS withdraws the proposed regulations or issues a notice of revised rulemaking, proposing substantial revisions in light of the comments received.

As a practical matter, given that DFS has already consulted with industry participants concerning the new rules prior to their publication, and given the emphasis that DFS and the Executive have placed on the necessity for these rules, it may be unlikely that any material changes will be forthcoming after Nov. 13.

That leaves the very real possibility that material questions and ambiguities concerning the regulations will remain, when they take effect as planned on Jan. 1, 2017. These include the following.

Who Is Covered?

The first question concerning the proposed regulations is to whom they apply and to what extent. By their terms, the rules apply to "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law." This covers traditional state-chartered banks and trust companies, as well as mortgage lenders and even check cashers. On its website, under the "Who We Supervise" link, DFS lists over 2,000 such entities. Add to this all insurers operating under the New York Insurance Law, and the list expands significantly.

> Described as "first in the nation," the draft regulations are sweeping in scope and reach well beyond core financial institutions, such as banks and lenders.

Confusion ensues, however, when an entity may fall under DFS supervision for a portion of its operations, but still thinks of itself as primarily or perhaps exclusively regulated by another agency. Take, for example, a federally chartered bank that also functions as a DFS-approved trust company. As such, the bank would be a "Covered Entity" and subject to the new regulations.

There, however, lies the rub. Do the new rules apply to the bank's entire operations, or only to the trust company portion of its business? Do the exemptions in the regulations based on size or revenue apply to the bank as a whole, or to its DFS-regulated activities only? And does such a distinction even make a difference, because it is unlikely that a bank has dedicated systems and security measures for its DFS-regulated operations.

The new rules provide no guidance on these issues, and the trend in cybersecurity regulation is for greater rather than narrower reach, as well as for overlapping concurrent jurisdiction. Without DFS clarification on this issue, a financial institution such as the one in our example will face the difficult decision of whether to apply DFS's new mandates to all of its business operations, or risk potential action by DFS for not doing so.

Employee Information

Broadly conceived, the draft regulations define four primary "buckets" of protected information: (i) business information, the compromise of which could have a material adverse effect on a Covered Entity; (ii) information acquired in the process of providing financial services or products to a customer; (iii) health care information; and (iv) any other information that can be used to distinguish or trace an individual's identity.

Only one of these "buckets" is conditioned on the manner in which the information is acquired: information acquired in the process of providing financial products or services to a

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.*

customer, which is broadly coterminous with the familiar definition of Nonpublic Personal Information (NPI) under the Gramm-Leach-Bliley Act. The remaining three "buckets" apply, regardless of where the information comes from or to whom it refers. For example, under the draft regulations, a Covered Entity would be required to protect the following categories of information to the same degree as customer NPI: employee W-2 data; employee health-care data; and employee emails, the disclosure of which could have a material adverse effect on the Covered Entity (as in the Sony Pictures breach).

As a practical matter, a Covered Entity may and likely should protect employee information as jealously as customer NPI, but the question remains what action DFS will take if a Covered Entity suffers a purely employee-related breach that has no material effect on the company's bottom line or customer NPI. As currently conceived, an entity experiencing such a breach would have 72 hours to disclose it to the Superintendent of DFS and be subject to enforcement, should its policies and practices in relation to the breached information prove to have been inadequate.

Cybersecurity Events

One area where DFS stands at the vanguard is in the 72-hour reporting window it proposes for any "Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information." "Cybersecurity Event" is defined as: "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."

This definition of "Cybersecurity Event" is staggeringly broad and nearly certainly encompasses more than DFS intended to target. Under this definition, most firewall denies and alerts from a Covered Entity's Intrusion Detection System /Intrusion Prevention System (IDS/IPS) would qualify as Cybersecurity Events. Yet firewall denies for even a mid-sized business entity with circa 200 users can run in the tens of thousands or more per month. IDS/IPS alerts can run in the millions per month.

Although not every Cybersecurity Event will be reportable, any Cybersecurity Event that has a "reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information" will be. It follows then that, if these provisions are adopted unaltered, every Covered Entity will have to have a system in place, no later than 180 days after the anticipated effective date of the regulations of Jan. 1, 2017, to discern between the deafening background noise of constant cyberattacks and those specific attacks that have a "reasonable likelihood" of having a material effect on the entity or any effect on Nonpublic Information, regardless of materiality. Again, as a practical matter, all financial institutions should likely have such a system in place. A primary function of information security is separating the material attacks from non-material attacks.

The complicating factor is the 72-hour reporting window, which—after all—is an outside deadline. The proposed regulations require notice to the Superintendent "as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event." In the fog of war surrounding a cybersecurity incident, speed can be an entity's worst enemy, however. Undue haste in labeling an incident as a breach, or classifying an incident as material, can set off a chain reaction of over-notification, increased expense, and increased exposure that any entity should seek to avoid.

It also remains to be seen how DFS will receive these notices, which will almost certainly be electronically, and to what extent DFS will be able to deal with the deluge of notices that are sure to come. Further, because of the short notification window, Covered Entities will likely have to keep their cybersecurity incident response teams (and any backup teams) on duty 24 hours a day, seven days a week, 365 days a year, which many Covered Entities may not be able to do. Notably, the size exemptions contained in the regulations do not release exempted entities from the 72-hour reporting duty.

Other Laws and Rules

The trend in cybersecurity regulation has been emulation and overlap. California's data breach notification law triggered 46 other states to enact similar laws in the last 13 years, with more states likely to follow. DFS's new regulations may spawn new rules in other jurisdictions, many of which are likely to overlap with existing rules, just as the DFS regulations overlap with the Gramm-Leach-Bliley Act, state breach notification laws, HIPAA (Health Insurance Portability and Accountability Act), and the FTC Act. And DFS's focus on substantive security measures such as multi-factor authentication or encryption both in transit and at rest will undoubtedly sway opinion on what cybersecurity measures are considered "reasonable" or "industry standard."

Guidance Is Needed

Guidance from DFS will be key to avoid undue burden and unintended consequences arising from the proposed regulations. The first form such guidance will take will be in the summary of comments and DFS's responses after expiration of the 45-day notice and comment period. It is unlikely, however, that this summary will answer every question or resolve every ambiguity in the proposed regulations. DFS will have to answer remaining questions as Covered Entities comply with the regulations, or such questions will be resolved in the courts or with additional administrative action.