FUND INTELLIGENCE
Compliance

Five takeaways from the lead-up to NY's cyber rule deadline

The two-year implementation period for the Department of Financial Services rule ends March 1.

David Isenberg February 22, 2019,

Following two years' worth of preparation, the implementation period for the **New York Department of Financial Services** first-in-the-nation cybersecurity rule will at last come to a close on March 1. Here are some of the biggest lessons that firms have taken away from it:

Small firms may be disproportionately affected

For most aspects of the regulation, sources confirmed that it has been harder to comply if you are a smaller firm, closely-held firm, or an individual business proprietor. "I think that large financial services firms have had an opportunity to see this coming down the pike— companies that have a robust compliance function," said **Daniel Rabinowitz**, partner at **Kramer Levin Naftalis & Frankel.**

Fortunately, because of the extensive publicity surrounding this regulation, sources expect that even smaller firms have been preparing for this implementation deadline, a process that can take a year to a year-and-a-half. "If you're a small business, there are resources out there in the marketplace in the way of consultants and best practices," said Rabinowitz.

Third-party vendors need to be compliant, even if not covered

While NYDFS does not have the authority to directly enforce against non-covered thirdparty vendors who handle digital information protected through cybersecurity, it can penalize covered entities if their vendors aren't compliant. "So the real governing factor on the vendors is the fact that a covered entity, if you're not complying with the regulation, might decide to use a different vendor," said **Mike Stiglianese**, managing director at **BDO New York**.

For Rabinowitz, this vendor issue gets complicated because the regulation is ambiguous as to what constitutes "information systems" of covered entities. "[D]oes that mean the information systems that it owns? Licenses? Sub-licenses? Licenses from a parent company? So there are some interpretive questions I think in addressing whose systems are we talking about and where those boundaries exist," Rabinowitz said.

The regulation requiring covered entities' third-party vendors be compliant could create various complications in the relationship between NYDFS covered entities and third-party vendors, so setting up clear expectations and disclosures can help. For Stiglianese, measures such as a written policy elucidating vendor obligations and a due diligence process established with the vendor can help maintain assurances that parties do have controls in place. Further, it is crucial that covered entities "[have] some sort of understanding of the data that every one of your vendors have. Understanding whether they have the type of nonpublic information that's covered by the regulation, how they handle it," Stiglianese said.

“If certain organizations have not done this process proactively, and they’re just notifying their vendors now, there may be a lot of surprised vendors out there,” Stiglianese said.

To Stiglianese, this has the potential to disproportionately affect smaller firms. “The more that they’re dealing with covered entities, the more likely they will be okay at this time. It’s the ones that are smaller in nature, in dealing with one or two of these along the way, that have the higher risk of being in the situation where they’re first finding out that this could have an impact on them. And if that covered entity has a significant part of their revenue, then that obviously has drastic impact on them,” said Stiglianese.

Even exempted entities must register for exempted status

The regulation requires that even regulatory-exempt entities must still register as exempt, potentially imposing further costs and confusion on exempted entities, which is arguably what the exemption was meant to mitigate. “If you have a license with the DFS to do any finance business, you have to comply with this regulation, absent certain exemptions. Presumably, if you’re a company that has a close call as to whether you may be doing business in New York, you’ve probably already addressed whether or not you have to get licensed,” said Rabinowitz.

One of the biggest groups of exempted entities from the regulation are licensed individuals who work for a licensed firm as an employee, receiving all of their clients (and their data) from their overlying employer. Once the employee begins moonlighting, or leaves the firm/company, they must become NYDFR compliant. “If you’re a broker acting in your own capacity and you’re not working for a company that’s not licensed, then you lose all that architecture,” said Rabinowitz.

Entities with only partial, or limited, exemption suffer the most, says Stiglianese. “They’re so small that they have this limited exemption, they don’t make a lot of money, but they’re still required to have some aspects of the regulation in place. So in their case, this is a true cost to them that they probably never factored into their business model,” Stiglianese said.

Rabinowitz concurs because employees, purportedly exempt from the non-self-effectuating regulation, must still register with the NYDFS as exempt. “It’s not altogether clear how employees get and preserve that exemption. It should be automatic. If the reg were drafted differently, it would say employees are exempted. But because the reg says employees are exempted from certain things and they have to file ‘within 30 days of the determination’ that you’re exempt, a somewhat passive way to put it, again they’re going into the portal and they’re finding that it’s not obvious which of these field the employees have to fill out and which ones they don’t have to fill out,” Rabinowitz said.

For Rabinowitz, the regulation could see an improvement on this. “I think people would like to see exemptions automatically self-effectuating, instead of something that you have to report.”

If you have had concerns or issues with the portal, you are not alone

One particularly frustrating aspect of NYDFS for Rabinowitz and his clients was the rather Kafkaesque portal. “[L]ike a lot of online portals you can’t view the whole thing until you go into it and start filling in the field. You have to do it iteratively. You reach inflection points where there’s not an obvious answer. I think there’s difficulty in navigating the form in a way that’s making people wonder if they’re compliant.”

“And we can’t see it because you have to be a licensed entity to get in the portal, so it’s not as though an outside lawyer or advisor can easily quarterback this for you. People filling it in have to make judgments,” Rabinowitz added.

This could even make some covered or exempt parties question whether they have followed the regulation or not. But Rabinowitz believes that the department will look at the substance of the reporting, not the minutiae. “I have to think that the DFS will be responsive about those kinds of questions and will focus on more substantive questions of [whether] people have appropriate controls, protocols, mechanism designed to foreclose breaches and data compromises and the like,” Rabinowitz said.

Enforcement will likely be flexible at first, looking at big picture

This substantive, qualitative approach to regulation fits into what sources say is NYDFS' overall prophylactic approach to cybersecurity compliance, rather than a prescriptive one.

However, participants shouldn't get too complacent. "Technically this is a law and if you're not in compliance, you're breaking the law," said Stiglianese. Whereas regulations like the EU's General Data Protection Regulation are also regulations, Stiglianese believes that NYDFS has less flexibility than others. "While [NYDFS is] more prescriptive than other guidances have been, and it is a regulation not a guidance, all of it is pretty much good cybersecurity hygiene," said Stiglianese.

One question that looms is what enforcement will look like. Rabinowitz believes that, based on the agency's previous behavior in this process, the agency will offer corrective opportunities before punitive measures. "I think if they find that people haven't made the appropriate certifications or have qualified them in a certain way they will reach out to those companies. And they will say to them do you want to correct this, do you want to supplement it? I don't see any penalties or severe consequences arising out of this initial phase unless a company does something egregious," said Rabinowitz.

"I'm not sure how they're going to address a second offender, and where they're going with actual examinations and doing the physical assessment of whether someone's in compliance or not," said Stiglianese.

And at the end of the day, both compliance officers for companies and regulators are not cybersecurity experts. But still, says Rabinowitz, "We're in wait-and-see mode."

Article re-print purchased from Fund Intelligence *https://fundintelligence.global/compliance/news/five-takeaways-from-the-lead-up-to-nys-cyber-rule-deadline/*