Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

NY Cybersecurity Rules Will Be Enforced As They Mature

By **Allison Grande**

Law360 (February 14, 2018, 11:01 PM EST) -- New York's financial regulator has been relatively quiet since first-of-their-kind cybersecurity rules took effect last year, but attorneys expect that the first wave of compliance certifications due Thursday and looming deadlines to implement more technically complex aspects of the regulation will trigger an enforcement blitz.

Banks, insurance companies, and other financial services institutions and licensees regulated by New York's Department of Financial Services have had to contend with the landmark cybersecurity rules since August, when the first implementation deadline hit. The inaugural round required business to adhere only to certain portions of the regulation, including the mandates to put a cybersecurity program in place, appoint a chief information security officer and report breaches within 72 hours.

While the department has maintained a low profile since the initial horn sounded, the disclosures that businesses are required to file by Thursday certifying their compliance with the portions of the regulation that are live so far, coupled with upcoming implementation rounds in March and September that cover safeguards such as risk assessments, multifactor authentication and encryption lead industry watchers to believe that the regulator won't lurk in the shadows for much longer.

"I think it's logical to assume that we're going to see some enforcement around these cyber regulations," said Celeste Koeleveld, a Clifford Chance LLP partner who up until January worked as DFS' general counsel and helped to draft the rules. "An agency like DFS and its Superintendent Maria Vullo are going to want to not only issue regulations, but also make sure they enforce them. It's hard for regulations to be effective unless an agency puts its enforcement might behind them."

The superintendent signaled last month that her office was still very much attuned to the cybersecurity regulations by issuing a press release on Jan. 22 reminding covered entities of the Feb. 15 deadline for electronically filing a certification of compliance for the previous calendar year. She also used the announcement to disclose for the first time that the department would be adding cybersecurity questions to its "first day letters," which are notices it issues to commence its examinations of financial services companies.

"The DFS compliance certification is a critical governance pillar for the cybersecurity program of all DFS regulated entities," Vullo said in her announcement last month, adding that "as DFS continues to implement its landmark cybersecurity regulation, we will take proactive steps to protect our financial services industry from cyber criminals."

Attorneys have been eyeing the first compliance certifications as an important indicator of how the department intends to enforce the novel cybersecurity requirements it has put in place.

"It will be interesting to note what, if any, action DFS takes for those entities who are unable to certify compliance in time," said Alexander Southwell, Gibson Dunn & Crutcher LLP's privacy, cybersecurity and consumer protection practice leader. "It would not surprise me to see DFS look to make an example of a company that hasn't certified compliance in order to convey the seriousness of these issues."

The certification, while seemingly routine, requires a great deal of investment and assumption of risk from both companies and the individual they choose to sign off on their compliance. Under the regulation, covered entities must conduct an annual review and assessment of the program's achievements, deficiencies and overall compliance with the regulatory standards that are thus far in place, and either the chairperson of the Board of Directors or a senior officer is responsible for certifying this compliance through a DFS portal.

"The certification requirement drives accountability," said Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP and chair of the firm's data security practice. "It underscores the responsibility that either a senior officer or board member is delegated to test for diligence the organization's compliance steps under the regulation."

The potential for enforcement is exacerbated by the black-and-white nature of the certification process: Either a company can certify they are in compliance, or they can't.

"One of the biggest challenges for companies right now and why this regulation is unique is that the certification doesn't allow for any wiggle room or for companies to say 'We're getting there or working on it,'" Ballard Spahr LLP of counsel Kim Phan said. "So a company, particularly a smaller one, that is struggling to put in place some of the new requirements is stuck."

The certification requirement provides DFS with what Phan said could be a "clear and easy tool" to bring enforcement action not just against companies that fail to certify, but against the individuals who sign off on certifications that are later found to be insufficient, attorneys noted.

"What has always been one of the more interesting aspects of the regulation is that it effectively requires a CISO or someone within the organization to put themselves on the line and say to DFS that the company is in compliance with the regulation," Morgan Lewis & Bockius LLP partner Charles M. Horn said. "In order for someone to step up to the plate like that, a lot of work needs to be done within the organization in terms of talking to people and learning about its cybersecurity posture."

The enterprise-wide effort necessary to determine compliance may lead a company to identify areas of improvement, but that may not necessarily bar certification, Mayer Brown LLP partner Jeffrey P. Taft said.

"Just because something can be improved doesn't necessarily mean you're not in compliance," he said, noting that each organization needs to determine what is an acceptable form of compliance for themselves and that companies would be wise to "create an internal record that shows how they were able to get to the point where they say that they're able to certify compliance."

The risk of enforcement isn't going to end with the certification process, and is likely to only get more intense as more aspects of the regulation take effect, attorneys were quick to note.

While the first round of provisions that went live in August raised some questions about the precise scope of the regulation and the exact methods for complying with these rules, attorneys for the most part agreed that the requirements were what Southwell described as "somewhat foundational" and relatively straightforward for companies that practice in this space.

"Putting a cybersecurity program in place, appointing a CISO, these are pretty basic things that most companies should have been thinking about and be comfortable with," Phan said.

However, future rounds contain tasks that are likely to require more time, money and technical expertise, making compliance and the resulting certifications trickier, according to attorneys.

"Overall, covered entities need to seriously address the issues and ensure they are on top of them well before the DFS' certification deadlines," Southwell said.

The next implementation deadline falls on March 1, when companies will need to have in place measures such as the completion of a risk assessment that will help inform their broader cybersecurity plans, multifactor authentication to verify users' identities, and vulnerability assessments to determine internal and external weaknesses.

Additional requirements such as encrypting sensitive data go into effect in September, and compliance with the entire regulation is expected by March 1, 2019.

While many of these requirements are quickly becoming industry standards and best practices, companies are likely to face challenges implementing them across their ecosystem and keeping up to date with the requirements, according to attorneys.

"We've seen some companies looking at legacy systems and having to make decisions about whether or not to migrate away from older systems that don't work effectively with encryption or multifactor authentication," said Edward McNicholas, co-leader of the privacy, data security and information law practice at Sidley Austin LLP. "The thing to remember about systems is that they are constantly aging, so making sure that systems are up to date and in compliance is really an ongoing process that doesn't have any particular deadline."

Aside from the implementation and compliance certification deadlines, financial institutions and insurers are also likely to face the risk enforcement during examinations, given the superintendent's revelation last month that the department would be adding questions related to cybersecurity to its opening letters.

"In light of that announcement, we can anticipate that examiners are going to go out and have a fairly long list of questions and will take cybersecurity issues seriously," Koeleveld said.

Horn noted that he expects DFS to be in more of a "listening and receiving mode" during the first examination cycle. It will likely be trying to get a sense of what regulated entities are doing to comply, but won't necessarily bring down the hammer at the outset "unless something egregious has happened and someone fell badly short of the mark," he said.

Liability risks will also spring up as more data breaches occur, due to the unprecedented and short 72-hour window that covered entities have to report such incidents. While the European Union will soon have a 72-hour notification deadline once the bloc's general data protection regulation takes effect in

March, none of the breach reporting laws on the books in 48 U.S. states have a reporting clock shorter than 45 days, and most don't set a specific timeframe for reporting.

"There are degrees to this that DFS may consider — it's one thing to file a notice within 96 hours, and it's another to file notice a month later," Taft said.

Koeleveld pointed out that DFS has "a history of graduated enforcement," meaning that they start with less serious violations and move up to more critical components of the regulation and increase the penalties accordingly, and she said she'd expect the department to take a similar approach to new cybersecurity rules.

"The department has made clear that they put the rules into effect because they had a real concern that the entities it supervises needed to do more to combat cyberthreats and they felt that just issuing guidance wasn't enough," she added. "Companies do cost-benefit analyses, and if something is guidance, they can say, 'That's nice but we'll get to it later.' A regulation makes it mandatory and gives it teeth."

Attorneys had predicted when the regulation was finalized last year that the rules would become a de facto national standard, and industry watchers said this week that they have observed companies rolling out certain mandates across the country instead of just targeting them to their operations within New York.

"For the most part, New York is becoming the tail that wags the dog in the sense that companies are employing the lowest common denominator approach in incorporating the rules across all of their operations," Taft said.

Other states, most notably Colorado and Vermont, are also moving toward implementing their own rules for certain financial institutions, especially in light of the headline-grabbing breach at Equifax that compromised 145.5 million individuals' personal data last year, and the National Association of Insurance Commissioners in October adopting a data security model law to serve as a template for other states to develop their own data security directives.

Given the growing risk of enforcement by the New York regulator and the increasing likelihood of other states following suit, attorneys recommend that companies in this space continue to closely monitor developments at both the state and federal levels and focus on how to best protect their systems from emerging cyberthreats.

"The hackers are and will be a much bigger threat than any set of regulations are, and companies should be designing their systems to protect against hackers," McNicholas said. "And if they're able to do so effectively, then they can essentially get compliance for free."

--Editing by Pamela Wilkinson.
