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 Spur Action But Not Uniformity

By **Allison Grande**

Law360, New York (March 9, 2017, 10:26 PM EST) -- Federal banking regulators, insurance commissioners and states from Connecticut to California will likely take up the mandates of a trailblazing cybersecurity regulation that recently took effect in New York. But they may be reluctant to hew too closely to New York's rules, which many consider to be overly stringent, even as they are under pressure to act in the face of mounting cyberthreats.

New rules developed by the New York Department of Financial Services, which went into effect on March 1, require banks, insurers, money businesses and regulated virtual currency operators to fortify their cybersecurity protocols by putting detailed data security programs in place, increasing their monitoring of third-party vendors, appointing chief information security officers and reporting breaches within 72 hours.

The set of rules has been called the first of its kind, but it almost certainly won't be the last with which financial institutions and insurers will have to grapple, experts say.

"In general, what we've seen recently in the cybersecurity space is what could be called 'regulatory group think,' and I think it's a given that these regulators are looking at what other regulators are doing and are taking their cues from each other," Debevoise & Plimpton LLP partner Jim Pastore said.

The enactment of New York's cybersecurity rules marks the culmination of years of work by the state's financial services regulator, studying cybersecurity issues and soliciting input on the most efficient and effective ways for banks and insurers to protect sensitive data from hackers. The push began under the department's first superintendent of financial services, Benjamin M. Lawsky, in the wake of major cybersecurity breaches at retailers like Target and Home Depot as well as banks such as JPMorgan Chase & Co., and has continued under current superintendent Maria T. Vullo.

Federal and state banking and insurance regulators feeling pressure to replace guidance and best practices with formalized rules in view of mounting data-security threats may find much to like about the New York regulations, given the significant work that went into developing them.

"The NYDFS may have a spillover effect as some of the standards may be adopted in other jurisdictions," Morgan Lewis & Bockius partner Mark Krotoski said.

However, the path to finalizing the New York regulations was not smooth, a factor that attorneys say

could give other regulators pause. Before adopting the cybersecurity rules verbatim, they will likely want to conduct their own investigations and come up with their own ideas on how to best protect consumer data.

New York's rules, initially floated in September, immediately came under fire for being too strict in mandating banks, insurers and a vast swath of other financial institutions to take prescriptive steps to protect against cyberattacks and quickly recover from data breaches.

In response, the department announced in December that it had decided to roll back the regulation slightly and give companies two extra months to comply. The revised rules eased some requirements for tasks such as encrypting data and breach notification, while retaining the spirit of many key obligations, including establishing and maintaining a comprehensive cybersecurity program.

"I think the New York regulations will be looked at in the future as how not to engage in cybersecurity regulation," Pillsbury Winthrop Shaw Pittman LLP partner Brian E. Finch said. He called the regulation "while surely well-intentioned … a mélange of basic security measures thrown together with no clear guidance on how they are supposed to work together or what would even constitute a sufficient or reasonable program for a covered entity to implement."

The result ends up being "this extremely difficult mixture of specific requirements and incredibly vague directions on how to successfully organize them," according to Finch.

"All that is guaranteed is that covered entities will be scrambling to determine how to put together a program their senior officers or board members can 'certify' to DFS," Finch said, referring to a much-maligned requirement starting in February 2018 that banks and insurers each year certify to the DFS their cybersecurity programs are in compliance with the new rules.

Krotoski said the controversy may prompt other regulators to shy away from following New York's rules too closely.

"Enforcers seeking to regulate cybersecurity matters must decide some initial fundamental policy questions," he said. "This includes whether to impose prescriptive standards or flexible guidelines and whether to create novel new standards or harmonize the regulations with existing cybersecurity standards.

"In our view, the NYDFS standards are overly prescriptive and impose novel standards that are costly and burdensome on covered entities and deprive them of needed flexibility," Krotoski said.

Finding new incentives to promote effective cybersecurity, rather than setting strict standards, may be the better approach for some regulators, he added.

"States should not follow the NYDFS cybersecurity rule because it is overly prescriptive and creates inconsistent standards with other existing cybersecurity standards," he said.

Some regulators around the country have already begun the typically lengthy process of delving into the cybersecurity landscape, with options at the state and federal levels for public entities to follow New York's lead.

The Federal Deposit Insurance Corp., the Federal Reserve Board and the Office of the Comptroller of the

Currency teamed up in October to release an advance notice of proposed rulemaking, inviting comment on enhanced cybersecurity risk-management standards that would apply to large and interconnected entities under their supervision.

The agencies sought input on more than three dozen questions, including whether they should issue a formal regulation, guidance or a combination of these approaches, or consider a two-tier approach that would impose higher standards for systems that provide key functionality to the financial sector. The comment period on these rules closed on Feb. 17, and the FDIC's records show that 24 comments were submitted.

The FDIC and Federal Reserve Board declined this week to comment on the proposed rulemaking, and the OCC could not be reached for comment. But attorneys say that they see many similarities between the federal regulators' proposal and what New York has done.

"It will not be surprising if future federal regulations incorporate many of the New York State provisions," Cullen and Dykman LLP partner Joseph D. Simon said, adding that New York "has a history of enacting financial service laws and regulations that are often adopted in some form at the federal level."

The National Association of Insurance Commissioners — whose members include DFS Superintendent Vullo, the representative for New York — is deeply entrenched in a process that the standards-setting body is hoping will result in a model law that each state would be free to adopt, outlining how insurers must safeguard consumers' information and respond in the event of a data breach.

The model law was first rolled out last March, and the NAIC has spent the past year working on revisions to address criticisms raised by insurance sector representatives, who say the model contains overly stringent notice requirements, and consumer advocates claiming it offers narrower protections for breach victims than existing state privacy laws.

Rhode Island Superintendent of Insurance Beth Dwyer, who is vice chair of the NAIC's cybersecurity working group, told Law360 this week that the process remains ongoing and that the small group of state insurance commissioners working on the model law recently released a third version, which is now open for public comment.

Dwyer noted that the next step for the model law — prompted in part by recent high-profile data breaches at health insurers Anthem Inc. and Premera Blue Cross — is uncertain, with the body considering a "number of different options," including sending the proposal to the larger innovation and technology task force or getting more input at the subgroup level.

"Even without a model in place, the NAIC has worked well in coordinating the commissioners of various states that have been affected by large data intrusions in the insurance industry in recent years," Dwyer said. "But a model rule would formalize that."

She stressed that coordination would be critical. "We wouldn't want 50 different commissioners doing 50 different things, so what's important here is to set out [the process] in as much detail as we can without knowing what the actual intrusion will be," she said.

Dwyer said the NAIC's model-rule makers have no plans at the moment to hew closely to New York's cybersecurity regulation, but she didn't close the door on the possibility that it would be influential.

"We're still working on a model rule that works for everyone and haven't gotten to the point yet of considering how to coordinate that with the New York rule," Dwyer said, adding that the group welcomed input from every state regulator — including the New York superintendent — on the proposal.

Like the insurance commissioners, banking regulators at the state level also are likely to be interested in formalizing cybersecurity guidance and best practices long observed in the industry, attorneys say.

"We hear about cyber breaches all the time, and I think that regulators want to stay out in front of it and protect their consumers," said JillAllison Opell, chair of Michelman & Robinson's insurance industry group.

Candidates to follow New York include what Pillsbury's Finch characterized as "the usual suspects" — Massachusetts, Connecticut, California, Maryland and Illinois.

"All of them have legislators and governors more interested in regulation than incentivizing secure behavior," Finch said.

Matt Smith, a spokesman for the Connecticut Department of Banking, recently told Law360 that cybersecurity has been a "top priority" for the agency and that the regulator remained "confident that our partnership with the banks, credit unions and other financial institutions we regulate addresses any concerns that all consumer information is protected and safeguarded."

Smith said the department was "unfamiliar with the New York proposal, as we were not consulted." He said the department was willing to take it into consideration as it continued taking steps to regulate cybersecurity issues.

"Once we review the [New York] proposal, we are open to adopting any provisions that may enhance our efforts and the risk profile of our institutions," Smith said.

Representatives for the banking regulators in California, Massachusetts, Maryland and Illinois did not immediately respond to a request for comment.

Cyberthreats from nation states and hacking groups show no signs of abating, and financial data continues to be an enticing target. Verizon's 2016 Data Breach Investigations Report found that 89 percent of breaches were financially motivated, according to Debevoise's Pastore. In the present circumstances, attorneys say there's little doubt that regulators across the country will be seeking to protect their citizens' data.

"For better or worse, once one person has gone ahead with it, it eliminates the caution or concern of being the first mover and makes it harder to defend why your state's citizens aren't being protected in the same way as others," Pastore said. "And as regulators get increasingly comfortable with cybersecurity as a topic, they're also likely to get increasingly comfortable with dictating more prescriptive regulation regarding technologies that have been found to reduce risk."

But while the new regulations may share similarities with what New York has done, it's more than likely that banks and insurers will soon find themselves contending with a sea of divergent rules similar to the ones that businesses must deal with now for reporting data breaches, an obligation that is dictated by

47 different state laws.

"There's a real possibility that much like the breach notification landscape, these covered entities may soon be staring down the barrel of a patchwork of regulation," Pastore said.

--Editing by Pamela Wilkinson and Jill Coffey.