CARLTON FIELDS

New York Eyes New Cybersecurity Rules for Banks and Vendors

November 27, 2015

Signs that New York state regulators may propose new cybersecurity rules are raising concerns that banks and their IT vendors could soon face more stringent reporting requirements — and that other states could follow suit. The New York Department of Financial Services (DFS) has not started a formal rulemaking proceeding. But acting New York Superintendent of Financial Services Anthony Albanese told federal banking regulators in a Nov. 9 letter that “there is a demonstrated need for robust regulatory action in the cyber security space” and said the agency is considering a number of requirements. Entities would be required to implement and maintain written cybersecurity policies and procedures, according to an outline of the proposed rules in the letter. A particular emphasis of any potential new rules could be bank vendors. Albanese said in his letter that a 2013 DFS survey of bank cybersecurity practices highlighted the financial industry's reliance on third-party service providers for critical banking and insurance functions as “a continuing challenge.” **More Specific Rules**

In the letter, Albanese said he wants to work with state and federal agencies “to develop a comprehensive cyber security framework that addresses the most critical issues, while still preserving the flexibility to address New York-specific concerns” and invited their feedback. A DFS spokeswoman said Albanese was seeking comments from the regulators before starting a formal rulemaking proceeding. The letter was sent to 20 agencies and regulatory associations, including the Federal Reserve, the Office of the Comptroller of the Currency, the Treasury Department, the Federal Deposit Insurance Corp., the Consumer Financial Protection Bureau and the National Credit Union Administration. Albanese's letter “could be a precursor to regulations,” the New York Bankers Association noted in a Nov. 19 statement to Bloomberg BNA, but said it “does not wish to speculate on what those regulations could contain or when they could be released.” The potential rules “would go beyond the regulatory requirements in other existing regimes” by imposing more specific rules, attorneys with Hogan Lovells LLP's cybersecurity practice said a Nov. 19 blog post. “For example, a regulatory requirement mandating that covered entities ensure that third parties encrypt sensitive

data at rest goes beyond what several other regulatory regimes have typically required," the blog post said. Another potential regulation that would require banks be indemnified in vendor contracts goes further in "potentially dictating what are typically commercially negotiated terms," the Hogan Lovells post said. **'Significant Effect.'**

Harriet Pearson, a partner at the firm, told Bloomberg BNA in a Nov. 20 e-mail that "some of the contemplated measures could have quite a significant effect." One potential regulation would require notifying the DFS of incidents with "a reasonable likelihood of materially affecting the normal operation of the entity" and for any incident where the regulated entity's board is notified. That could have the unintended effect of discouraging communications with the board, "stifling productive conversations about risk management between management and directors," said Pearson, who co-chairs the Georgetown Cybersecurity Law Institute. "Such a patchwork will divert resources from organizations' core cybersecurity risk management efforts," she said. "I do not see an immediate rush for states to adopt such regulations, but New York state is a very important jurisdiction, so efforts there are important to monitor," Pearson said. Craig Carpenter, a data privacy and cybersecurity attorney with Thompson & Knight LLP, said many of the issues raised in the DFS letter, such as requiring a written cybersecurity plan or expectations from vendors, are already covered by state or federal regulations. But he said that New York's early proposals "go a step beyond many of the existing, vague regulations to require specific cybersecurity 'best practices' by including, for example, detailed descriptions of the required contents of a company's cybersecurity policy and vendor agreements and requiring encryption of data at rest and specific penetration and vulnerability testing requirements." The biggest impact, however, may not be on financial institutions that are used to being regulated "but the potential for this trend in specific cybersecurity requirements bleeding over into other industries that are not as accustomed to regulatory oversight," Carpenter said. **No Big Change?**

Todd Hinnen, a partner with the Perkins Coie and a former acting assistant attorney general for national security, said he expects less of an impact on banks since federal and state regulators already require them to have a cybersecurity plan. To guard against potential litigation, "companies should be conducting appropriate diligence regarding vendors' security practices and ensuring that their contracts with their vendors allocate responsibility (and potential liability) for data security incidents appropriately," Hinnen said in a Nov. 19 e-mail to Bloomberg BNA. "In short, they are things financial institutions should be doing anyway." The fact that the DFS wants to collaborate with federal regulators is a "hopeful sign" the agency will end up deciding more regulations aren't needed, according to Doug Johnson, senior vice president of payments and cybersecurity policy at the American Bankers Association. Federal regulations already require such things as creating a cybersecurity plan and monitoring of contractors, he said in a Nov. 19 interview with Bloomberg BNA. "If there's any gap which is not already being fulfilled by financial regulatory agencies, I would hope that New York will find that there isn't a necessity to create a different program." **Already Regulated**

Joseph Swanson, securities litigation counsel at Carlton Fields, said in a Nov. 19 interview he agrees with the DFS letter's point that banks are increasingly being targeted for cybercrimes. "Where we

think the letter is troubling is the premise that there's a need for more robust regulations in this space," he said." The market is already taking care of this. Entities and banks are already aware of the risks they face. They're ahead of the curve in staying ahead of threats and responding to attacks. What we can easily predict is there will be ambiguities in whatever laws are promulgated." Some potential rules Albanese identified would be difficult to enforce, Swanson said, such as a requirement that IT staff be up to date on the latest cybersecurity threats and responses. Rules "conceivably saying what contracts [with vendors] must contain" would go further than the usual regulatory approach of letting private parties negotiate contracts on their own, he said.

Related Practices

Technology
Cybersecurity and Privacy
Financial Services Regulatory
Consumer Finance

Related Industries

Technology