Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Lawsky Speech Portends Strict NY Cybersecurity Standards

Law360, New York (February 27, 2015, 4:47 PM ET) --

Alexander H. Southwell

On Feb. 25, 2015, Superintendent Benjamin M. Lawsky of the New York Department of Financial Services gave a speech at Columbia Law School titled "Financial Federalism: The Catalytic Role of State Regulators in a Post-Financial Crisis World." In the speech, Lawsky advocated a role of states as agents for regulatory change to address emerging risks — taking into consideration initiatives at the federal level, but not waiting for federal regulators to take the lead.

Lawsky further explained the concept of "financial federalism" by describing how it impacts three areas of DFS focus: (1) Wall Street accountability in the wake of the financial crisis, (2) anti-money laundering efforts in the financial sector, and (3) strengthening cybersecurity in the financial markets.

Calling cybersecurity the "most important issue that [DFS] will face in 2015," Lawsky explained that New York's financial regulator is focused on developing "concrete actions" to strengthen cybersecurity at the institutions regulated by DFS. He highlighted three key initiatives: (1) revising regular examinations of banks and insurance companies to include targeted assessments of cybersecurity preparedness; (2) addressing the cybersecurity of third-party vendors; and (3) support for use of multifactor authentication. The initiatives, together with the emphasis on the role of states as reformers, leaves little doubt that DFS will take a proactive approach to regulating cybersecurity practices, as it has in other areas.

Revised Regular Examinations to Include Targeted Assessments of Cybersecurity Preparedness

Of the three initiatives discussed by Lawsky, the changes to the examination process have been developed the most. Indeed, the momentum behind these changes dates back to 2013, when DFS first sent inquiries to regulated banks and insurance companies requesting information on their cybersecurity policies and procedures.

Changes to the examination process for the banking sector have been under consideration since the spring of 2014, when Gov. Andrew Cuomo released a report detailing the growing risk and sophistication of cyberattacks facing New York banks. In conjunction with the release, the governor directed DFS to conduct new, regular, targeted cybersecurity preparedness assessments of the banks regulated by DFS

in order to “better safeguard financial institutions from attacks and secure personal bank records from being breached.”

On Dec. 10, 2014, Lawsky issued an industry guidance letter to all DFS-regulated banks that outlined the specific issues and factors that would be included in the new targeted assessments of cybersecurity preparedness. The underlying goal of the new assessments is to prompt regulated entities to consider cybersecurity “as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology.”

To achieve that end, bank examinations were expanded to include, among others, assessments of protocols for the detection of cybersecurity breaches and penetration testing, corporate governance related to cybersecurity, defenses against cybersecurity breaches (including multifactor authentication, which is discussed in a separate initiative below), and the security of third-party vendors (which is also discussed separately below).

The revised DFS targeted assessments of cybersecurity practices that Lawsky discussed relating to regulated banks formally commenced upon publication of the industry guidance letter in December 2014. However, it is possible that there may be further changes to the targeted assessments of cybersecurity preparedness.

In addition, DFS has also focused on targeted cybersecurity assessments for insurance companies. On Feb. 8, 2015, DFS released a report on cybersecurity in the insurance industry. The report includes the results of 2013 and 2014 DFS cybersecurity surveys of regulated insurance companies. These survey results and related analysis will be used by DFS to integrate regular, targeted assessments of cybersecurity preparedness at insurance companies, likely in a similar manner as discussed above for the regulated banking sector.

As Lawsky said in his speech, the premise behind these targeted assessments is straightforward: “if [DFS] grade[s] banks and insurers directly on their defenses against hackers as part of [their] examinations, it will incentivize those companies to prioritize and shore up their cyber security protections.”

Vulnerabilities with Third-Party Vendors

Superintendent Lawsky also noted concern about cybersecurity risks arising from third-party vendors of financial institutions. Noting that banks and insurance companies often rely on third-party vendors for a wide range of services, Lawsky warned that such vendors may present a possible “backdoor” entrance for malicious actors if the vendors had access to a financial institution’s information technology systems and had inadequate cybersecurity protections. The superintendent indicated that he was considering a mandate requiring a minimum level of contractual representations and warranties financial institutions would have to receive from third-party vendors. This would include representations and warranties related to critical cybersecurity measures.

Based on Lawsky’s speech, it does not appear that DFS will differentiate between different types of vendors: he provided examples of third-party vendors that included law firms providing legal advice as well as companies providing facilities maintenance.

The superintendent appears to be seeking to use these mandates as “tough medicine” to encourage vendors to strengthen their cybersecurity or face the loss of financial institution clients. While it is

undisputed that vulnerabilities in the cybersecurity practices of third-party vendors have led to significant breaches in companies, such regulation could require third-party vendors in sectors far from the regulatory purview of the DFS to effectively comply with stringent cybersecurity requirements in order to continue to service customers in the regulated financial industry.

Multifactor Authentication

In his speech, Lawsky also discussed the inherent limitations of a username and password system to verify identities. Instead, he advocated for a multifactor authentication system. Although the method may vary, such systems require more than one form of authentication to verify the legitimacy of the user. Because of this additional layer of authentication, they are considered more secure than a traditional username and password combination.

Lawsky revealed that the DFS is considering adopting regulations that would mandate the use of multifactor authentication by financial institutions. If enacted, this would make the DFS the first regulator to require such systems, although many financial institutions already utilize such authentication systems.

Conclusion

Focusing his discussion of cybersecurity on three areas the DFS has identified as critical to the future cybersecurity practices of financial institutions, Lawsky advanced his view that states can play a "catalytic" role in raising national and international cybersecurity practices. While recognizing that federal action has a place on this issues, the superintendent sees New York as an "incubator[] for new approaches to vexing problems" and a potential leader in establishing heightened cybersecurity requirements through financial regulations. This philosophy animates his identification of targeted cybersecurity preparedness assessments, vulnerabilities with third-party vendors, and the use of multifactor authentication as critical areas in which New York will seek to play a role.

Time will tell if these initiatives in fact stimulate similar cybersecurity regulations in other states (or at the federal level), but it is clear the DFS will continue to push for higher cybersecurity standards among financial institutions under Lawsky's leadership.

—By Alexander H. Southwell, Adam Chen and Stephenie Gosnell Handler, Gibson Dunn & Crutcher LLP

Alexander Southwell is a partner and Adam Chen is an associate in Gibson Dunn's New York office. Stephenie Gosnell Handler is an associate in Washington, D.C.