CARLTON FIELDS

New York's Banking Regulator Proposes Tougher Anti-Money Laundering and Cybersecurity Enforcement Rules

March 23, 2015

"Ineffective regulation can sometimes be worse than no regulation at all since it breeds a false sense of security."

> —Benjamin Lawsky, New York State Superintendent of Financial Services in a February 25, speech entitled "Financial Federalism: The Catalytic Role of State Regulators in a Post-Financial Crisis World."

The New York Department of Financial Services (DFS) supervises all New York State chartered banks, most U.S.-based branches and agencies of foreign banking institutions, and all insurance companies in New York. The DFS also supervises providers of financial services such as mortgage bankers and check cashing stores. Its superintendent, Benjamin Lawsky, takes a tough stance on regulations directed at the financial services sector. Recently, in remarks made at Columbia University, Mr. Lawsky noted that, because they deal with extremely broad issues, federal regulators have not been effective in dealing with wrongdoing on Wall Street. To combat ineffectual federal regulation, he proposed "Financial Federalism," and called for state regulators to impose stricter controls on the financial industry than those imposed by the federal government. Mr. Lawsky's vision of Financial Federalism has three prongs:

- Greater Wall Street accountability
- Preventing money laundering in the financial sector
- Strengthening cyber security in financial markets

Wall Street

Mr. Lawsky, a firm believer that real fraud deterrence on Wall Street will require individual liability and

accountability, emphasized the need to make individuals responsible for wrongdoing face "real consequences." As such, he called for regulators to work harder to identify individual wrongdoers.

Preventing Money Laundering

Mr. Lawsky said the DFS wants greater controls on automatic transaction monitoring and filtering systems ("AML controls"), noting that every day, hundreds of millions of transactions through the bank payments system move hundreds of billions of dollars around the globe. Because banks rely on AML controls to track evidence of criminal activity, two potential problems arise. First, AML controls could be inadequate, defective, or improperly managed by the employees responsible for their operation. Worse still, these controls are susceptible to employee malfeasance or willful blindness, i.e., employees can manipulate controls to allow suspicious transactions to go through AML controls undetected. As a result, DFS is considering implementing random audits of AML controls as well as advocating for independent monitors to audit and examine controls instead of self-reporting. Second, DFS is proposing that senior executives must personally attest to the adequacy and robustness of AML control systems. This idea is modeled after Section 302 of Sarbanes-Oxley 2002, which requires the CEO and CFO of publicly traded companies to attest to the truthfulness and adequacy of company financial statements. **Cybersecurity**

Fearing that the financial sector will suffer a major cyber-attack (Mr. Lawsky refers to this as "Cyber 9/11"), DFS will revamp examinations of banks and insurance companies to incorporate new, targeted assessments of cybersecurity preparedness. Next, DFS is considering steps to address the cybersecurity of third-party vendors. Because third-party vendors have access to a financial institution's information technology, DFS has contemplated mandating that financial institutions require robust representations and warranties from third-party vendors regarding cybersecurity. Finally, Mr. Lawsky suggested all firms should move to "multi-factor authentication," which adds a second layer of security beyond the username and password. Upon entering a username and password, an additional password, required for access, is generated and sent to a cell phone.

Conclusion

Given Mr. Lawsky's remarks it seems clear executives can expect to be subject to more personal liability. Further, regulated entities and third-party vendors must be prepared to spend more money, time, and personnel on AML controls and cybersecurity measures.

Related Practices

Consumer Finance
Consumer Finance
Cybersecurity and Privacy
Life, Annuity, and Retirement Litigation
Financial Services Regulatory
White Collar Crime & Government Investigations
Securities Litigation and Enforcement