COMPLIANCE & ENFORCEMENT

Program on Corporate Compliance and Enforcement at New York University School of Law

With Cybercrime on the Rise, Financial Regulators Advance Stricter Cybersecurity Regulations

Courtesy of **John F. Savarese** and **Marshall L. Miller**

As ever-increasing cyber attacks target companies in the financial sector and beyond, financial regulators in New York and Washington, D.C. have focused their attention on cybersecurity risk. On October 19, federal banking regulators sought comments, due January 17, 2017, on enhanced cyber risk-management standards for major financial institutions. Meanwhile, the New York State Department of Financial Services (DFS) recently announced detailed regulations, requiring covered institutions — entities authorized under New York State banking, insurance, or financial services laws —to meet strict minimum cybersecurity standards. And yesterday, the Department of Treasury's Financial Crimes Enforcement Network (FinCEN) issued an advisory on the reporting of cyber events under the Bank Secrecy Act.

The DFS rules, which require compliance within 180 days of their January 1, 2017 effective date and contain phase-in periods for certain provisions, require the protection of "nonpublic information," broadly defined to range from sensitive business information to information "linked or linkable" to an individual. To achieve such protection, the regulations require the adoption of formal cybersecurity programs that perform core functions: identifying cyber risks; protecting against, detecting, responding to, and recovering from cybersecurity events; and meeting regulatory reporting obligations. In a break from prior standards, the regulations also mandate specific policies, including the encryption of nonpublic information both in transit and at rest, the implementation of audit trail systems, and the performance of annual penetration testing and quarterly vulnerability assessments.

The responsibility to institute the policies required by DFS rests squarely on senior officers and boards of directors. At least annually— and as frequently as necessary to address evolving risks— boards of directors of covered institutions will be required to review, and senior officers to approve, written cybersecurity policies. Covered institutions will also be required to employ Chief Information Security Officers, who, in turn, must provide boards with cybersecurity reports, available to DFS upon request; board chairs or senior officers must file

compliance certifications with DFS, with false certifications carrying potential civil and criminal penalties.

The DFS regulations' government-notification requirements also sweep more broadly than existing disclosure rules. Covered institutions will be required to notify DFS within 72 hours of any cybersecurity event— defined to include an attempt as well as a successful attack— where that event impacts nonpublic information or is likely to materially affect operations. This requirement raises concerns that notification will be required not only far more frequently, but also before the nature, scope, and effects of the cybersecurity event are fully understood. DFS should mitigate these concerns by assuring covered institutions that notifications will not be required until initial investigations reveal the contours of cybersecurity events, including any effects on nonpublic information and operations.

While the new DFS regulations will take effect in January, federal regulators are at an earlier stage in the rulemaking process. Last week, the Federal Reserve, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency jointly issued a notice of rulemaking, signaling their intention to impose enhanced cybersecurity standards on sector-critical firms and the nation's largest financial institutions — those with assets of $50 billion or more — with even stricter standards applied to those institutions' "sector-critical systems." Federal

regulators are engaging in a two-step process, with comments on this initial notice informing a more detailed proposal, to be circulated for further public comment in 2017.

Federal regulators are still evaluating what framework to apply to cybersecurity regulation, contemplating options ranging from an enhanced, high-level risk-management framework to a more directive regulation with granular policy requirements, akin to the DFS approach. Notably, federal regulators appear to be pursuing an enhanced role for boards of directors, soliciting feedback on proposals to require that boards approve and oversee cyber risk-management strategy, receive direct reports from cybersecurity officers, and have access to appropriate cybersecurity expertise.

Yesterday, FinCEN joined the regulatory conversation, issuing an advisory that directs financial institutions to file Suspicious Activity Reports (SARs) regarding cyber events, defined as attempts to compromise or gain unauthorized access to electronic systems or information, that they suspect were intended to affect transactions involving $5,000 or more. The advisory expressly applies not only to cyber events that directly target such transactions, but also to events involving sensitive data, like customer information, that could be used to affect such transactions in the future. In addition, the advisory requires institutions to include cyber-related information in all

SARs — whether related to a cyber event or not — and encourages institutions to share such information internally and throughout the financial sector.

Financial institutions are on the front line — not only for cyber attack, but also for regulatory oversight and enforcement. Companies regulated by DFS must move swiftly to ensure compliance with its new regulations; the nation's largest financial institutions and sector-critical firms should take care to monitor and comment on the developing federal rules; and all financial institutions will need to bring SAR reporting into the cyber age. Meanwhile, corporations across all industries would be wise to pay close attention, as these new cyber rules are likely to serve as models for regulators outside the financial sector, influence emerging codes of conduct, and contribute to the ongoing evolution of best practices in the cybersecurity space.

John F. Savarese is a partner in the Litigation Department of Wachtell, Lipton, Rosen & Katz. **Marshall L. Miller** is Of Counsel at Wachtell, Lipton, Rosen & Katz.

*The above post was originally issued as a **Wachtell, Lipton, Rosen & Katz** memo by **John F. Savarese**, **David M. Silk**, **Wayne M. Carlin**, **Sabastian V. Niles**, **Marshall L. Miller**, and **Jorge M. Gutierrez, Jr.***

Disclaimer

This entry was posted in Cybersecurity and tagged John Savarese, Marshall L. Miller on October 28, 2016 [https://wp.nyu.edu/compliance_enforcement/2016/10/28/with-cybercrime-on-the-rise-financial-regulators-advance-stricter-cybersecurity-regulations/] by Serina M. Vash.