OUTSIDE COUNSEL

Financial Institutions: Are You Ready for Your Cyber-Exam?

John Curran and Marc J. Armas, New York Law Journal

June 15, 2017

John Curran and Marc J. Armas

With the increased visibility and impact of cyber-attacks on financial institutions, regulators and other enforcement authorities are enhancing the cybersecurity requirements for the financial services industry. The New York State Department of Financial Services (DFS) has taken a leadership role by imposing specific "minimum standards" for regulated institutions. These standards are intended to address the risks to customer information and the integrity of core banking infrastructure, for which persistent vulnerabilities implicate the very safety and soundness of the broader financial system.

These risks materialized most clearly in the heist at Central Bank of Bangladesh last year, whereby hackers gained access to the bank's SWIFT messaging system and sent fraudulent wire payments totaling close to $1 billion—$80 million of which were successful. This attack was not isolated. Most recently, on April 10, 2017, the Wall Street Journal reported additional details regarding the elaborate attempted cyber heist of the Union Bank of India in July 2016. Fortunately, quick detection of the malware prevented a loss of close to $170 million. Reports note the similarities in

malware used in the attacks on the Union Bank of India and the February 2016 theft from the Bangladesh Central Bank. Some reports have linked the hacking tools used in these bank compromises to those used by North Korea to attack Sony Pictures in 2014 in response to the release of the movie "The Interview."

In the context of these devastating cyber-attacks, DFS issued Cybersecurity Regulations that took effect on March 1, 2017. These "first-in-the-nation" regulations require financial services organizations to develop and maintain robust cybersecurity programs to better secure consumer data and preserve the overall health of the financial services industry.[1] Gov. Andrew Cuomo announced that the new regulations "will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cyber-crimes."[2]

Certain provisions of the new cybersecurity regulations are effective immediately, while the remaining provisions will become effective in stages.[3] DFS regulates banking institutions as well as insurance companies, trusts, credit unions, and charities.

The regulations set forth detailed requirements that institutions must follow, including:

• Establishing a cyber security program "designed to protect the confidentiality, integrity and availability" of the institution's information systems;

• Conducting a cyber risk assessment;

• Implementing a Board of Director approved written Cybersecurity Policy;

• Appointing a Chief Information Security Officer;

• Implementing Access and Monitoring Controls;

• Performing Third Party Diligence; and

• Creating a rigorous Incident Response Plan

Perhaps most significantly, the new Regulations require notice to DFS within 72 hours of a "cybersecurity event" and an Annual Certification of compliance with the DFS Cybersecurity Regulations by the Board or a senior official of the Financial Institution.[4]

Although DFS provides a "grace period" for up to an additional two years for certain requirements, covered institutions must file their first certification of compliance by Feb. 15, 2018. For many institutions, the time to act is now, especially since we expect other regulators to follow the lead of DFS.

Addressing DFS and other regulatory cyber requirements is not simply a "technical" challenge. Successful compliance will only be ensured, and adequately documented and communicated, when General and Financial Crime Compliance Counsel play an integral role in the institutions' readiness efforts.

Affected institutions should take steps now to ensure they are ready not only for the first certification, but for the regulatory examinations by DFS and other agencies that will doubtless

come in the years ahead. Specifically, financial institutions should consider focusing on the following priorities:

• Putting in place a "cyber-readiness" team with appropriate governance and reporting structures in order to identify issues, track gaps, and define next steps with timelines;

• Performing a cyber health check or "gap analysis" against the regulatory requirements;

• Stress testing the health check by a qualified external firm;

• Regularly updating senior executives and the Board on gaps and mitigating controls; and

• Monitoring and testing the controls, including tests of the effectiveness of the Incident Response plan through "table top exercises"

Meeting regulatory obligations for cybersecurity is a classic compliance challenge. A successful readiness program must leverage the diverse skill sets, regulatory mindset, and expertise of counsel who address other financial compliance issues such as anti-money laundering, sanctions, and corruption on a daily basis.

---

1. Press Release, New York State Department of Financial Services, Governor Cuomo Announces First-In-The-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions From Cyber Attacks to Take Effect March 1 (Feb 16, 2017).

2. Id.

3. Id.

4. This requirement is in addition to the FINCEN requirements that financial institutions file Suspicious Activity Reports for Cyber Incidents.

John Curran is a partner, and Marc J. Armas an associate, at Walden Macht & Haran.