CLIENT ALERT

NYDFS Implements First-In-The-Nation Cybersecurity Rule for Covered Financial Services Companies

Feb.28.2017

On February 16, 2017, the New York Department of Financial Services (NYDFS) published a final rule (the "Rule") imposing new cybersecurity requirements on covered financial institutions. The Rule takes effect on March 1, 2017; however, covered institutions will have 180 days to come into compliance with most requirements, with longer transition periods of 1-2 years for certain obligations. The Rule requires covered entities to certify annually that they are in compliance with its requirements, with the first certification due on February 15, 2018. NYDFS revised its prior drafts of the Rule based on two rounds of public comment.

The Rule is notable for its potentially broad reach. Specifically, the Rule defines a "Covered Entity" as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization" under New York's Banking Law, Insurance Law, or Financial Services Law. (Sec. 500.01(c)). While the Rule contains exemptions based on, for example, number of employees (fewer than 10); gross annual revenue (less than $5 million in each of the last three fiscal years from New York business operations of the Covered Entity and any affiliates); and year-end total assets (less than $10 million, including assets of all affiliates), it nevertheless potentially draws a broad range of banks, insurance companies, and other financial services providers within its reach. (Sec. 500.19).

The Rule requires Covered Entities to establish and maintain a risk-based cybersecurity program that is "designed to protect the confidentiality, integrity and availability" of its information systems, as well as any "nonpublic information" stored on such systems. (Sec. 500.02). It likewise requires Covered Entities to prepare written policies, and to designate a Chief Information Security Officer (CISO). (Secs. 500.03 and 500.04). Among the other requirements the Rule imposes are:

- Either "effective continuous monitoring" of the Covered Entity's information system or annual penetration testing and bi-annual vulnerability assessments, consistent with the Entity's level of risk. (Sec. 500.05)
- Systems that are designed to reconstruct material financial transactions sufficient to support normal obligations of the Entity and that include audit trails designed to detect and respond to cybersecurity events. (Sec. 500.06)
- Development of third-party service provider security policies that set forth minimum cybersecurity practices required to be met by third parties providing services to the Covered Entity. (Sec. 500.11)
- The use of multi-factor authentication, consistent with the Entity's risk assessment, in order to prevent unauthorized access to nonpublic information or information systems. (Sec. 500.12)
- The use of encryption, consistent with the Entity's risk assessment, in order to protect nonpublic information held or transmitted by the Entity "both in transit over external networks and at rest." (Sec. 500.15)
- A requirement to provide the NYDFS Superintendent with notice within 72 hours from a determination that a qualifying cybersecurity event has occurred. (Sec. 500.17(a))

- An annual reporting requirement to the NYDFS Superintendent certifying compliance with the Rule and setting forth any identified areas, systems, or processes requiring material improvement, updating, or redesign, and documenting any remedial efforts planned or underway to address these. Entities also must retain for inspection all records, schedules, and data supporting the certification, for period of five years. (Sec. 500.17(b))

The Rule is the first known effort by a state regulatory agency to impose mandatory cybersecurity requirements on a class of businesses, and in that way it represents a break from prior efforts that have focused more on voluntary standards. New York's experience with the implementation of the Rule may inform similar efforts by other state regulators in the future.

Institutions that are already subject to other obligatory cybersecurity standards for the financial industry, such as those imposed under the Gramm-Leach Bliley Act (GLBA), or by the Financial Industry Regulatory Authority (FINRA) or the Securities and Exchange Commission's Office of Compliance, Inspections and Examinations (SEC OCIE), may find that they already have addressed many of the steps required by the new Rule. However, they still will have to assess for any overlaps and gaps with the requirements of the new Rule as they build compliance programs. The Rule's impact is likely to be most prominently felt by financial services companies that are not already subject to federal cybersecurity standards, to the extent they have not already established cybersecurity programs that are largely compliant.

It is also unclear how the Rule—and others like it that may appear in the future—will interact with voluntary standards aimed at critical infrastructure more generally, such as the National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF). While the Rule addresses many of the same considerations as other pre-existing standards, it delves deeper into the specifics. For example, multi-factor authentication and encryption at rest are tools that industry can use to meet standards such as the GLBA and NIST CSF, but neither is specifically required. Given the increasing interrelationship between state and federal obligations, as well as both cybersecurity and anti-money laundering (AML) regulations, it is important for affected firms to adopt a coordinated approach with an integrated team of legal professionals. Crowell and Moring's Privacy and Cybersecurity and AML practices are happy to provide further guidance in each of these areas.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Carlton Greene
Partner – Washington, D.C.
Phone: +1 202.624.2818
Email: cgreene@crowell.com

Maida Oringher Lerner
Senior Counsel – Washington, D.C.
Phone: +1 202.624.2596
Email: mlerner@crowell.com

Kate M. Growley, CIPP/G, CIPP/US

Partner – Washington, D.C.
Phone: +1 202.624.2698
Email: kgrowley@crowell.com