FISH & RICHARDSON

IP Litigation **White Collar**

Tough New Cybersecurity Regulations from the New York Department of Financial Services Go Live

March 2, 2017

Back to Fish's Litigation Blog

Yesterday, March 1, 2017, marked the effective date of a set of cybersecurity regulations promulgated by the New York Department of Financial Services (NYFDS) for the banking, insurance, and financial sectors operating in the State of New York. The regulations set substantive data security requirements for all financial institutions, and make New York the first state in the nation to mandate minimum cybersecurity standards. Given the prominence of these entities in New York, industry players, commentators, federal and other state regulators, and even Congress will be watching the implementation of these regulations with keen interest.

Who's Covered?

These "first-in-the-nation" cybersecurity regulations, promulgated at 23 NYCRR 500, apply to all entities operating in New York under authorization under the Banking Law, the Insurance Law, and the Financial Services Law ("Covered Entities"). The regulations, revised in response to second round comments, clarifiy that a Covered Entity is exempt from certain provisions if it has:

- fewer than 10 employees, including independent contractors or affiliates, located in New York or responsible for business of the entity;
- less than $5 million in gross revenue in each of the last three fiscal years from its and its affiliates New York business operations; or
- less than $10 million in year-end total assets, including assets of all affiliates.

23 NYCRR 500.19(a). Exemptions from certain provisions are also available for certain entities that do not handle classes of nonpublic information. 23 NYCRR 500.19(c), (d). But note, if an entity determines that it is exempt, it nonetheless must file a Notice of Exemption within 30 days of that determination. 23 NYCRR 500.19(e).

What is Required?

The final regulations are sweeping and granular at the same time. One major requirement is that entities conduct a **periodic risk assessment** to inform management as to the particular cyber and data risks of the organization, including how they evolve over time. The regulations contemplate that this risk assessment will "inform the design of the cybersecurity program." 23 NYCRR 500.09(a).

Based on the risk assessment, entities are required to implement a **cybersecurity program** and create a written set of **cybersecurity policies** designed to protect the entity's information systems and its data from cyberthreats, and to detect, respond, and recover from cyberattacks. 23 NYCRR 500.02, 500.03. The cybersecurity program is required to cover policies and procedures for:

- multi-factor authentication;
- data retention limitations;
- training and monitoring of personnel;
- encryption (or alternative controls) of nonpublic information in transit and at rest; and
- an incident response plan.

23 NYCRR 500.12-16. Reflecting the NYFDS's interest in maintaining the integrity and functionality of the financial sector, the regulations go considerably beyond protecting personally-identifiable information and other non-public information. The regulations prod Covered Entities to consider their cyber risks in areas such as "business continuity," "disaster recovery," and "systems operations and availability concerns." 23 NYCRR 500.03(e), (f). After implementation, the cybersecurity program is either to be **continuously monitored**, or else periodically subject to **penetration tests and vulnerability assessments**. 23 NYCRR 500.05. Periodic assessments and reviews are also required as to **access privileges**, **application security** policies, and the risk presented by **third party service providers**.

Another headline is the required designation of a **Chief Information Security Officer** (CISO), who may be an employee or a third party service provider. The CISO is required by the regulations to report at least annually to the Board of Directors, a nod to the growing consensus that cybersecurity is a board-level concern and ranks high on the list of enterprise priorities with which the Board should be fully engaged. 23 NYCRR 500.04.

Finally, the regulations require prompt, **72-hour notice** to the Superintendent of "cybersecurity events" impacting the organization that are otherwise reportable under existing law or regulation, or reasonably likely to "materially" impact the organization's business operations. 23 NYCRR 500.17(a). Notably, the definition of a "cybersecurity event" includes even unsuccessful attempts, 23 NYCRR 500.01(d)—making the materiality standard key, since it ameliorates the otherwise overwhelming burden of reporting every single unsuccessful attempt to breach an organization's cyber-defenses. Annual self-certifications are also required, beginning February 15, 2018. 23 NYCRR 500.17(b).

Even entities who are exempt from most of the regulations' provisions cannot escape conducting the risk assessment, establishing policies for third-party service provider and data retention, and submitting breach and annual notice requirements to the Superintendent.

Reactions?

The current version of the regulations has undergone two rounds of public comment since the first iteration was published in September 2016. Unsurprisingly, industry concerns arose that the regulations were too burdensome and unrealistic, especially with regard to timing. While certain requirements relaxed over the notice and comment process, the sheer comprehensiveness and detail in the regulations stay largely intact. Here are some takeaways:

Takeaway 1: Tight Deadlines for Compliance

Covered entities need to move fast. Some requirements are due within 180 days, and the first self-certification of compliance is due by February 15, 2018. The heart of the regulations—establishment of the cybersecurity program—must be in place by August 28, 2017. And while other deadlines look a little more distant, such as the one-year deadline for the risk assessment, the distance may be illusory: the design of the cybersecurity program is, by regulation, informed by the risk assessment.

A quick-glance schedule of compliance can be found below:

Date of Compliance	Requirements In Place
August 28, 2017	o Cybersecurity Program o Cybersecurity Policy o Designation of Chief Information Security Officer o Access Privileges o Cybersecurity Personnel and Intelligence o Incident Response Plan
February 15, 2018	o First Annual Certification of Compliance*
March 1, 2018	o Penetration Testing and Vulnerability Assessments o Risk Assessment* o Multi-Factor Authentication o Training Program o Chief Information Security Officer Report to Board
September 1, 2018	o Audit Trail o Application Security

	o Limitations on Data Retention* o Monitoring Program o Encryption of Nonpublic Information
March 1, 2019	o Third Party Service Provider Security Policy*

**- No Covered Entity is exempted from these requirements.*

Takeaway 2: Neither "One-Size-Fits-All" nor "Set It and Forget It"

One of the earlier complaints of the initial iteration of the regulations was that it mandated a "one-size-fits-all" cybersecurity policy. Heeding industry concerns, the NYFDS has adopted a more flexible, risk-based approach, expressly keying off many of the cybersecurity program requirements to the required risk assessment (but see odd timing, above).

Similarly, the requirement that the risk assessment be conducted periodically ensures that an organization's cybersecurity program does not stagnate in the face of evolving business operations or evolving cyberthreats—no "set it and forget it."

Takeaway 3: The Spill-Over Effect

NYFDS intends for these new cybersecurity requirements to raise standards well beyond the financial sector. The regulations mandate that entities assess the risk of their third party service providers, and implement written policies to ensure that they adhere to minimum cybersecurity measures if the entities' sensitive systems and nonpublic information are at risk. The enormous leverage that large banks and financial services firms have over their vendors—including accounting firms, information technology companies, data storage companies, and even law firms—no doubt will hasten improvement in their own cybersecurity programs.

Related Tags

cybersecurity White Collar New York Department of Financial Services NYFDS

Blog Authors

Caroline K. Simons | Principal

Caroline Simons is a Principal in the Boston office of Fish & Richardson. She serves clients in the areas of white collar defense, internal investigations, cybersecurity, and complex civil litigation. Ms. Simons strives at the outset to understand her clients' businesses,...

Claire Collins | Associate

Claire Collins is a litigation associate in Fish & Richardson's Boston office. During law school, Ms. Collins was a legal intern for the Middlesex District Attorney's Office. She has experience researching and drafting motions and legal memorandums.

Gus P. Coldebella | Principal

Gus P. Coldebella, a member of the National Law Journal's inaugural class of "Cybersecurity Trailblazers" in 2015, is a principal in the Commercial Litigation Group in Fish's Boston and Washington, D.C. offices. His practice involves helping companies deal with all aspects of...

Leave a Reply