PRIMER ON THE NEW NYDFS CYBERSECURITY REGULATION

BY JEEWON KIM SERRATO, COUNSEL AND REENA SAHNI, PARTNER AT SHEARMAN & STERLING LLP.

The New York Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies (the Final Regulation)[1] took effect on March 1, 2017. We discussed in our earlier publication the background on how the original proposal of the regulation was updated in the context of other recent developments in the financial services industry.[2] In the introductory section (§ 500.00) of the Final Regulation, the NYDFS stated that: "The financial services industry is a significant target of cybersecurity threats…Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted… Adoption of the program outlined in these regulations is a priority for New York State."

The NYDFS regulation confirms once more how cybersecurity concerns are at the top of the agenda of priorities for many state and federal regulators in the banking and financial services industry. Pursuant to the Final Regulation, certain banks, insurers and other financial services institutions holding a New York state license will be required to conduct periodic assessments of their cybersecurity risks and implement and maintain a cybersecurity program designed to address such risks.

Who is affected?

The regulation applies to any entity that holds a certificate, permit, accreditation or similar authorization under banking, insurance or financial services laws (each, a covered entity). The definition appears to be broad, especially considering that the concept of "similar authorization" may apply to service providers and/or independent contractors of covered entities operating under any relevant certificate or permit required by New York banking, insurance or financial services law.

Affiliates and extraterrestrial research

Comment letters on the Original Proposed Regulation raised concerns with respect to the extraterritorial scope – in particular with respect to the broad definition of foreign banking organizations (FBOs).

In response, the NYDFS clarified that a New York branch of a foreign bank falls within the definition of covered entity, and therefore is subject to the applicable cybersecurity requirements. In addition, the Final Regulation provides that a covered entity can satisfy the applicable cybersecurity requirements by adopting a cybersecurity program maintained by an affiliate (defined in § 500.01) provided that the affiliate's program is compliant with the applicable cybersecurity requirements introduced by the NYDFS. Therefore, under the Final Regulation, the New York branch of an FBO may comply with the newly introduced cybersecurity requirements either by:

- Establishing and maintaining its own cybersecurity program, or
- Adopting the program of the FBO itself, if it is compliant with the regulation.

Exemptions

The Final Regulation includes an exemption from some of the cybersecurity requirements for covered entities whose number of employees, revenues and assets do not exceed certain thresholds. Covered entities meeting any of the following criteria are exempted from a number of cybersecurity requirements under the Final Regulation (including the requirements to appoint a CISO, encrypt non-public information, and adopt an incident response plan):

- Fewer than 10 employees, including any independent contractors of the covered entity or its affiliates located in New York or responsible for business of the covered entity

> "The financial services industry is a significant target of cybersecurity threats …given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted."
>
> The New York Department of Financial Services

1 Available at http: http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf (23 N.Y.C.R.R. pt. 500).
2 Available at http://www.shearman.com/en/newsinsights/publications/2017/01/cybersecurity-protection-of-financial-data

- Less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the covered entity and its affiliates
- Less than $10,000,000 in year-end total assets, calculated in accordance with GAAP, including assets of all Affiliates

In addition, the limited exemption applicable to covered entities with less than $5 million in gross revenue for each of the last three fiscal years is now further expanded to include covered entities with less than $5 million in gross revenue "from its New York business operations (or its affiliates' operations)." Therefore, certain larger financial institutions with smaller New York operations may now qualify for either of these new exemptions. Each covered entity that qualifies for the exemption above is required to file a Notice of Exemption with the NYDFS.

Timeline for compliance

The regulation went into effect on March 1, 2017. Pursuant to the Final Regulation, each Covered Entity is required to establish and maintain a cybersecurity program tailored to address the certain critical cybersecurity concerns by August 28, 2017 (180 days from the effective date). This program should include the following elements, among others:

- Written cybersecurity policy (§ 500.03)
- Appointment of a chief information security officer (CISO) (§ 500.04(a)) and additional cybersecurity personnel (§ 500.10)
- Access privileges to protect non-public information (§ 500.07) Incident response plan designed to promptly respond to a cybersecurity event (§ 500.16)
- Procedures to promptly notify NYDFS of any cybersecurity events (§ 500.17)

One of the main changes from earlier proposals is that the Final Regulation allows for a more flexible and risk-based approach. Compared to the Original Proposed Regulation, which drew criticism because it was seen as a one-size-fits-all approach, the covered entity's cybersecurity program may now use risk assessments to identify the particular risks that are relevant to its business operations and assess the availability and effectiveness of controls that are designed to respond to those threats. Each covered entity is required to conduct the risk assessment periodically (and not annually as provided for by the Original Proposed Regulation).

The implementation of the program will provide covered entities with the foundation for a robust and successful plan to protect against cyber threats.

CISO report, testing and training

A number of requirements detailed in the Final Regulation have a 12-month transition period for covered entities to comply. These requirements must be met by March 1, 2018:

- CISO report on the covered entity's program (§ 500.04(b))
- Testing and vulnerability assessments (§ 500.05)
- Periodic risk assessments (§ 500.09)
- Multi-factor authentication to protect non-public information (§ 500.12)
- Cybersecurity awareness training for all personnel (§ 500.14(b))

Cybersecurity risks and third-party service providers

Further requirements of the Final Regulation have an 18-month transitional period for compliance and must be implemented by September 1, 2018. These include:

- Audit trail (§ 500.06)
- Application security policies for the development of in-house applications (§ 500.08)
- Data retention policies (§ 500.13)
- Monitoring of authorized users (§ 500.14(a))
- Encryption of nonpublic information (§ 500.15)

Risk management for third-party service providers

The Final Regulation specifically addresses scenarios under which third-party service providers have access or hold non-public information pertaining to a covered entity (§ 500.11). Covered entities will have until March 1, 2019 (two years from the effective date) to implement policies related to third-party service providers.

In those circumstances, a covered entity is required to implement written policies and procedures to ensure the security and integrity of such non-public information, by providing for:

- Minimum cybersecurity practices to be met by third-party service providers
- Due diligence processes to evaluate the adequacy of the cybersecurity practices of third-party service providers
- Periodic assessments of third-party service providers from a cybersecurity risk management perspective

Conclusion

The cybersecurity regulation adopted by the NYDFS imposes significant new requirements and obligations on covered entities. In light of the 180-day compliance window and the staggered implementation schedule, covered entities should immediately begin assessing their cybersecurity risks, implementing effective policies and developing robust cybersecurity programs to achieve compliance with the new cybersecurity requirements.

Part of the Mergermarket Group

www.mergermarketgroup.com

330 Hudson St. FL 4
New York, NY 10013
USA

t: +1 212.686.5606
f: +1 212.686.2664
sales.us@mergermarket.com

10 Queen Street Place
London
EC4R 1BE
United Kingdom

t: +44 (0)20 7059 6100
f: +44 (0)20 7059 6101
sales@mergermarket.com

Suite 1602-6
Grand Millennium Plaza
181 Queen's Road, Central
Hong Kong

t: +852 2158 9700
f: +852 2158 9701
sales.asia@mergermarket.com