New York Revises Proposed Cybersecurity Regulations, Pushes Back Effective Date

By: Jay Shapiro and Laura Schmidt
Cyber Law and Data Protection Alert
1.3.17

After receiving strong criticism from the banking and insurance industries, the New York State Department of Financial Services (NYDFS) has issued updated proposed cybersecurity regulations and pushed back the effective date of the regulations from January 1, 2017 to March 1, 2017. The updated proposed regulations adopt a softer tone that provides for greater flexibility in crafting and maintaining a cybersecurity program.

As previously noted (see New York State Proposes New Cybersecurity Regulations), NYDFS proposed regulations last fall that would require banks, insurance companies and financial institutions that it regulates to adopt and maintain a cybersecurity program that protects customer information and the information technology systems. The original proposed regulations were complex and would have required regulated companies to adopt specific technological standards, such as encryption and multi-factor authentication. During the 45-day notice and public comment period, NYDFS received extensive comments and complaints from banks, insurers and others that the proposed regulations did not distinguish between financial institutions of different sizes and imposed onerous requirements that did not reflect the variation in risks that different companies face.

Under the updated proposed regulations, companies regulated by NYDFS would still be required to establish a cybersecurity policy, maintain a cybersecurity program, and designate a Chief Information Security Officer (CISO) responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policy. However, the revised regulations are more flexible and accommodating for regulated organizations.

Most importantly for smaller banks, insurance companies, and financial services companies, NYDFS adjusted the exemptions to the proposed regulations. Under the original regulations, regulated companies with less than 1,000 customers in each of the last three calendar years would be exempt from certain parts of the regulation. The updated proposed regulations have changed the "1,000 customer" exemption to provide that companies with less than 10 employees (including independent contractors) are exempt from complying with more onerous parts of the regulations. However, even companies that fall within this exemption would still have to comply with certain parts of the regulations, such as maintaining a cybersecurity policy, adopting a cybersecurity program, and limiting access privileges.

The revised proposed regulations also now provide a partial exemption for regulated entities that do not directly or indirectly operate or maintain, utilize, or control any information systems and are not required to, directly or indirectly, control, own, access, generate, receive or possess nonpublic information. Again, such entities would still be required to comply with certain parts of the regulations, such as implementing written policies and procedures for third party service providers and limiting data retention.

In part, the moderation in the regulations may very well have been the result of NYDFS acknowledging that implementing all of the components of such complex cybersecurity regulations would be time consuming, because the proposed regulations now provide for additional "transitional periods" for regulated entities to implement particular portions of the regulations. Regulated companies will have one year from the effective date of the regulations to: (1) create a report, authored by the CISO, on the entity's cybersecurity program and material cybersecurity risks; (2) conduct penetration testing and vulnerability assessments; (3) conduct a risk assessment of the entity's information systems; (4) implement multi-factor authentication; and (5) provide regular cybersecurity

training. Regulated companies will have eighteen months to: (1) establish audit trails; (2) impose application security; (3) craft policies and procedures for limiting data retention; (4) implement monitoring of access to nonpublic information; and (5) encrypt nonpublic information. Two years after the effective date, regulated entities will have to implement written policies and procedures designed to address third party service providers.

The revised proposed regulations also take a more relaxed stance on notification of cybersecurity events. The original proposed regulations required regulated entities to notify the NYDFS superintendent as promptly as possible, but in no event later than 72 hours "after becoming aware of a cybersecurity event," as defined by the regulations. As we noted when the original proposed regulations were released, this is a very short period of time to disclose a cybersecurity event to a government official. Furthermore, the original proposed regulations required regulated entities to report the actual *or potential* unauthorized tampering with or access to nonpublic information. The updated proposed regulations still hold on to the 72 hour time frame for reporting a cybersecurity event, but no longer require regulated entities to notify the superintendent of actual or potential unauthorized tampering to nonpublic information. Instead, notification would be required if "[e]vents…have a reasonable likelihood of materially harming any material part of the normal operation (s)" of the regulated entity.

The updated proposed regulations also allow more flexibility for companies, particularly in the technical aspects of the regulations that were previously imposed. For example, the initial version of the regulations required annual penetration testing and vulnerability assessments of information systems. The regulations now provide that regulated entities must include monitoring and testing designed to assess the effectiveness of the cybersecurity program, which can consist of continuous monitoring and periodic testing and vulnerability assessments or, alternatively, annual penetration testing and bi-annual vulnerability assessment. The updated proposed regulations would still require companies to maintain systems that can establish an audit trail if necessary, but no longer require companies to incorporate specific steps, such as tracking and data logging of all privileged authorized users access to critical systems. Finally, the updated regulations no longer require regulated entities to transition to encryption of nonpublic information that is at rest or in transit if the regulated entity is using effective alternative controls to protect nonpublic information. Under the earlier version of the regulations, companies were allowed to use alternative measures to secure nonpublic information, but were required to transition to encryption at a certain point.

In summary, the revised proposed regulations suggest that NYDFS heard the concerns and complaints of those in the banking and insurance industries. However, the revised regulations also demonstrate that NYDFS is not going to abandon its efforts to establish minimum regulatory standards that require banks, insurance companies and financial service companies to create robust and multifaceted cybersecurity programs. While more flexible, the revised proposed regulations are still complex. Companies now have more time to become compliant, but should nevertheless recognize that outside legal and cybersecurity experts may be valuable assets in their efforts to ensure that the programs and policies implemented comply with these regulations.

If you have questions or would like additional information, please contact Jay Shapiro (shapiroj@whiteandwilliams.com; 212.714.3063) or another member of our Cyber Law and Data Protection Group.