Advisory

JANUARY 2017

If you have any questions about this Advisory, please contact:

CYBERSECURITY AND PRIVACY PRACTICE GROUP

MICHELLE DEBARGE
860.297.3702
mdebarge@wiggin.com

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

TIMOTHY WRIGHT
203.498.4340
twright@wiggin.com

INSURANCE PRACTICE GROUP

JOSEPH GRASSO
215.988.8312
jgrasso@wiggin.com

MICHAEL MENAPACE
860.297.3733
mmenapace@wiggin.com

Although Delayed, New York's Aggressive Cybersecurity Law Expected to Affect Financial Services and Insurance Firms

The regulatory environment for cybersecurity is rapidly changing, and state legislatures are not waiting for Congress to act. On December 28, 2016, the New York State Department of Financial Services ("NYDFS") revised **a proposed** rule that imposes new cybersecurity requirements on individuals and entities operating under the New York banking law, insurance law, or financial services law ("covered entities"). Don't stop reading if your company is not a covered entity, because the regulation also burdens third party providers with downstream requirements. Importantly, the rule covers nonpublic information, which is broader than you think. It includes personal information, health data, and sensitive business information. Although the proposed rule was expected to be implemented on January 1, 2017, it has been delayed two months and is currently in a final 30-day comment period. The final rule—which may be different than the revised proposed rule—will now become effective on March 1, 2017. Entities have 180 days after the effective date to comply. Depending on how NYDFS addresses comments from the public, the final rule is poised to become one of the most detailed and aggressive cyber laws in the country.

Broadly speaking, the rule requires covered entities to establish comprehensive data security programs, draft written policies, hire adequate personnel, and report any incidents within 72 hours. Additional requirements include maintaining detailed records and preserving data logs. The detailed nature of the requirements draws immediate similarities to the NIST Security Framework, which is increasingly becoming the industry standard for data security programs. But, as discussed below, some elements of the rule are new and go far beyond what it required of financial institutions under existing law. Many institutions, however, may already be addressing these requirements, but it is important for covered entitles to review the law in detail to ensure that they are in compliance. It would be a mistake, for example, for a covered entity to assume that because it has Gramm-Leach-Bliley-based data security measures in place, the NYDFS rule can be ignored.

IMPORTANT ELEMENTS OF THE PROPOSED NY RULE

1. Cybersecurity Program

The proposed rule requires covered entities to establish a "cybersecurity program" that preserves the confidentiality of their information and assesses risk. At a minimum, the program needs to identify internal and external cyber risks, protect an entity's nonpublic information and information systems, detect and respond to cybersecurity events, and fulfill reporting requirements. Additionally, the program needs to include (1) annual penetration testing, (2) audit trail systems, (3) limits on user access and data retention, (4) personnel training, and (5) multifactor authentication.

2. Cybersecurity Policy

A key component of the cybersecurity program is a written cybersecurity policy that lays out all of the company's data-related procedures. Be aware, the policy

CONTINUED ON NEXT PAGE

must go beyond a simple recitation of physical and technical safeguards that the company has implemented. Among other things, the policy must address risk assessment, data governance, data classification, vendor provider management, and incident response. After a policy is formulated, a senior officer or the company's board of directors needs to approve the policy.

3. Designation of a Chief Information Security Officer

Recognizing the importance of top-down leadership, NYDFS also included a provision in the rule requiring covered entities to designate a Chief Information Security Officer (CISO). A CISO is tasked with "overseeing and implementing the . . . cybersecurity program and enforcing [the] cybersecurity policy." The regulation permits a company to outsource the role to a third party, subject to certain conditions.

4. Third-Party Service Provider Requirements

Similar to other state and federal laws and regulations, the rule also addresses cyber risks in a company's supply chain. Covered entities must implement policies and procedures to ensure that third-party service providers are adequately protecting nonpublic information. These polices need to include:

- A risk assessment of third parties;
- Minimum cybersecurity practices required to be met by third parties;
- Due diligence to evaluate the adequacy of third-party cybersecurity practices; and
- Periodic assessments of the adequacy of third-party practices.

Furthermore, covered entities need to include provisions in third-party contracts that address, if applicable, (1) multifactor authentication, (2) encryption technologies, (3) notification requirements following a breach, and (4) additional representations and warranties covering cybersecurity.

5. Incident Reports

Perhaps the most onerous—and controversial—requirement, covered entities must report to the Superintendent of Financial Services within 72 hours after discovering an incident. An incident refers to any event that is required to be reported under existing law or "that has a reasonable likelihood of materially harming any material part of the normal operation of the Covered Entity." This requirement suggests that the entity must report information without having a complete understanding of what happened, what data was disclosed, and whether the breach was contained.

HOW DOES THE PROPOSED RULE DIFFER FROM EXISTING LAWS?

As it stands now, New York's proposed rule is a significant departure from existing federal law. By way of background, there are several regulations that currently affect financial institutions. Regulation S-P of the Securities and Exchange Commission, which implements the Security Rule of the Gramm-Leach-Bliley Act (GLBA), requires registered advisors, broker-dealers, private funds, and other financial institutions to develop adequate physical, administrative, and technical safeguards to protect customer information. Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) requires public companies to assess their "internal

CONTINUED ON NEXT PAGE

Although Delayed, New York's Aggressive Cybersecurity Law Expected to Affect Financial Services and Insurance Firms

controls," including IT controls, that protect their financial reporting and accounting. Also, the Financial Industry Regulatory Authority mandates that its members establish supervisory controls to ensure they are complying with applicable laws, including Regulation S-P. Lastly, New York has another data-related law; most New York companies must securely destroy records containing a customer's personal information when the records are no longer needed.

The proposed rule goes much further than these existing regulations. First, the scope of the covered data is much broader. As discussed above, the rule covers "nonpublic information," which includes certain nonpublic personal information, health information, and business information, whereas Regulation S-P and New York's data destruction law only cover a customer's personal information. Second, the proposed rule imposes a more detailed cybersecurity program. Conversely, Regulation S-P allows entities to design their own programs as long as they ensure the confidentiality of consumer records and protect against threats and unauthorized access. Moreover, other major elements of the rule, including the designation of a CISO, are completely new.

WHAT SHOULD COVERED ENTITIES DO?

Assuming the NYDFS proposed rule becomes final without meaningful changes, covered entities should take proactive steps now to ensure compliance.

- Determine if your company is covered under the rule.
- Compare the rule's requirements against those under existing laws to discern what additional steps your company must take to comply.
- Tailor your existing cybersecurity policy and program to align with the particular specifications of the rule.
- If you don't already have one, designate someone to act as CISO. That person will be instrumental in managing a cybersecurity policy and program, and should be involved in the planning process.
- Review your service vendor and provider arrangements, and determine which third parties will be covered and determine how to cover them contractually and operationally. Some contracts may need to be amended to address compliance with the rule.
- Also, as noted above, because the NIST Framework is increasingly being used as an industry benchmark, consider adding any additional features to meet the Framework's requirements.
- Confirm that your insurance coverage adequately covers cyber threats and data breaches.

For more information on New York's proposed rule, please contact Michelle DeBarge, John Kennedy, or Timothy Wright.