Bond

INFORMATION MEMO
CYBERSECURITY

AUGUST 28, 2018

Deadline Approaches for Major New Requirements under New York's Cybersecurity Rule

New York's cybersecurity regulations ("Regulations") set forth rolling deadlines, with some of the most significant mandates coming into play on September 1, 2018. Issued by the Department of Financial Services ("DFS"), and effective on March 2017, the Regulations apply to all entities licensed or regulated by DFS, including but not limited to banks, mortgage lenders, insurance companies and health plans in New York State ("Covered Entities").

General Requirements

Overall, the Regulations, among the most prescriptive in the nation, require Covered Entities to:

- Adopt a written cybersecurity policy setting forth policies and procedures for the protection of their information systems and broadly defined nonpublic information protected under the Regulations ("Nonpublic Information");
- Designate a qualified individual to serve as Chief Information Security Officer responsible for overseeing, implementing, and enforcing the cybersecurity program and policy; and
- Adopt policies and procedures designed to ensure the security of Nonpublic Information accessible to, or held by, third parties.

The New Mandates

The specific requirements that must be in met by September 1 are as follows:

- **Audit Trail –** Covered Entities must begin to maintain an audit trail that allows them to reconstruct material financial transactions to support normal operations in the event of a breach. Audit trails must also be useful in detecting and responding to cybersecurity events. Audit trail records permitting the reconstruction of financial transactions must be maintained for 5 years and those used to detect and respond to cybersecurity events must be kept for 3 years. (23 N.Y.C.R.R. § 500.06)
- **Application Security –** Covered Entities' cybersecurity programs must now include written procedures, guidelines and standards for the in-house development of software and procedures for testing the security of externally developed applications. (23 N.Y.C.R.R. § 500.08)
- **Limitations of Data Retention –** Covered Entities must adopt procedures for the periodic disposal of Nonpublic Information that is no longer necessary for business operations or other legitimate purposes of the Covered Entity, except where that information must otherwise be maintained by law or regulation or where targeted disposal is not reasonably feasible due to the manner of maintaining the information. (23 N.Y.C.R.R. § 500.13)
- **Monitoring –** Covered Entities must implement risk-based policies and controls designed to monitor activities of authorized users to detect unauthorized access, use of or tampering with Nonpublic Information by authorized users. (23 N.Y.C.R.R. § 500.14(a))

- **Training –** Covered Entities must provide regular cybersecurity awareness training for all personnel, updated as necessary to reflect risks identified by the Covered Entity in its periodic risk assessments. (23 N.Y.C.R.R. § 500.14(a))
- **Encryption of Nonpublic Information –** Nonpublic Information must now be encrypted both in transit and at rest, however alternative compensating measures are permitted where encryption is not feasible. (23 N.Y.C.R.R. § 500.15)

Breadth of the Encryption Requirement

The encryption requirement is broad and applies to all Nonpublic Information in a Covered Entity's possession. The Regulations define Nonpublic Information as:

1. Business-related information of a Covered Entity which if tampered with, or subject to unauthorized disclosure, access or use, would cause a material adverse impact to the business, operations, or security of the Covered Entity;
2. Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;
3. Any information or data, except age or gender, in any form or medium, created by or derived from a health care provider or an individual and that relates to: (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual. (23 N.Y.C.R.R. § 500.01(g))

Covered Entities must determine what data falls into the first category of Nonpublic Information based on their risk assessments. Nonpublic Information as defined above in the latter two categories must be encrypted. However, the regulations permit the Chief Information Security Officer to authorize effective alternative compensating controls for the Covered Entity, where encryption would not be feasible.

Certification of Compliance

On February 15, 2018, Covered Entities were required to certify to DFS that they were in compliance with those portions of the Regulations then in effect. The next annual certification deadline is February 15, 2019. A Covered Entity's board of directors, or a senior officer, will be required to execute a certificate of compliance on or before that date which certifies compliance with each applicable requirement of the Regulations.

Limited Exemptions May Apply to New Mandates

The requirements that become effective under the Regulations on September 1 are among the most challenging, costly, and demanding to implement. For example, encryption requires in the first instance the identification of all Nonpublic Information transmitted and stored by the Covered Entity. Audit trails must be targeted based on the risk assessment and should be established to yield the information that organizations need both to detect an intruder and track access in the wake of a breach. Small Covered Entities—those with fewer than 10 employees, less than $5 million in gross annual revenue or less than $10 million in assets—can apply for a limited exemption. Under the limited exemption, small Covered Entities are still bound by the data retention provision of the new mandates, but not the encryption, audit trail, application security, and monitoring requirements. (23 N.Y.C.R.R. § 500.19(a))

On the Horizon – Oversight of Third Party Service Providers

Under the Regulations, Covered Entities will soon be required to implement written policies and procedures governing their practices with respect to third party service providers that access Nonpublic Information ("Contractors") based on the Covered Entity's risk assessment. Specifically, as set forth in the Regulations, Covered Entities must adopt policies that address:

- Identification and risk assessment of Contractors;
- Minimum security practices that must be met by Contractors in order to do business with the Covered Entity;
- Procedures for due diligence to evaluate the adequacy of Contractors' security practices; and
- Guidelines for contractual protections relating to Contractors' access to Nonpublic Information.

Consistent with a risk assessment by the Covered Entity, such policies must address Contractors' procedures for access control, including multi-factor identification, encryption of information in transit and at rest, and practices to notify the Covered Entity of a cybersecurity event that directly impacts the Covered Entity's information systems and Nonpublic Information. Guidelines must also cover the representations and warranties that Contractors will extend to the Covered Entity regarding their cybersecurity policies.

For questions about the Cybersecurity Rule and steps required to achieve compliance, contact Tracy Miller, Co-Chair Cybersecurity and Data Privacy Practice Group, Curtis Johnson, or the attorney in our firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS

Bond, Schoeneck & King PLLC (Bond, we, or us), has prepared this communication to present only general information. This is not intended as legal advice, nor should you consider it as such. You should not act, or decline to act, based upon the contents. While we try to make sure that the information is complete and accurate, laws can change quickly. You should always formally engage a lawyer of your choosing before taking actions which have legal consequences. For information about our firm, practice areas and attorneys, visit our website, www.bsk.com. • Attorney Advertising • © 2018 Bond, Schoeneck & King PLLC, One Lincoln Center, Syracuse, NY 13202 • 315.218.8000.

CONNECT WITH US ON LINKEDIN: SEARCH FOR BOND, SCHOENECK & KING, PLLC

FOLLOW US ON TWITTER: SEARCH FOR BONDLAWFIRM