ALERT MEMORANDUM - MARCH 3, 2017

LEGAL UPDATE

New York Cybersecurity Regulations for Financial Institutions Enter Into Effect

While the New York Cybersecurity Regulations represent a softening in key respects from the requirements set forth in the initial proposal, the regulations impose minimum standards that exceed existing federal standards and introduce new requirements, including obligations to critically evaluate cybersecurity practices to ensure compliance, maintain detailed documentation demonstrating compliance and report cyber events to the New York Department of Financial Services.

If you have any questions concerning this memo, please reach out to your regular firm contacts or:

Michael Krimminger
T: +1 202 974 1720
mkrimminger@cgsh.com

Jonathan Kolodner
T: +1 212 225 2690
jkolodner@cgsh.com

Daniel Ilan
T: +1 212 225 2415
dilan@cgsh.com

The full text of the final Regulations can be accessed via this link: *https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf*

OVERVIEW

On March 1, 2017, the New York Department of Financial Services' (**DFS**) Cybersecurity Regulations (the **Regulations**) entered into effect.[1] Under the Regulations, any individual or non-governmental partnership, corporation, branch, agency, association or other entity operating under a license, registration, charter, certificate, permit, accreditation or similar authorization under New York banking, insurance or financial services laws (with narrow exceptions described below) (**Covered Entities**) is required to formally assess its cybersecurity risks and establish and maintain a cybersecurity program designed to address such risks in a "robust" fashion.

The Regulations are a direct response to the increasing number of cyber-attacks on insurers and financial institutions, such as the 2015 cyber-attack on Anthem, Inc. in which 78 million unencrypted records containing personal information were stolen and the 2016 cyber-attack on the central bank of Bangladesh in which stolen SWIFT credentials and malware were used to illegally transfer $81 million of funds held at the Federal Reserve Bank of New York.

These Regulations represent the first comprehensive state regulations to address cybersecurity threats. Under the Regulations, Covered Entities must comply with a number of detailed requirements, the majority of which are already practiced by Covered Entities that are subject to the Gramm-Leach-Bliley Act (**GLBA**), the federal statute regulating the collection, use, protection and disclosure of non-public personal information by financial institutions. For example, the Regulations essentially duplicate the mandate under the GLBA that requires Covered Entities to implement a comprehensive written information security program. However, some requirements of the Regulations exceed the minimum standards established by GLBA or constitute entirely new obligations, discussed in detail below.

This alert memorandum highlights some key terms of the Regulations, as well as key changes from the DFS's initial proposed regulations issued on September 13, 2016 and discussed in our alert memo "New York Regulators Propose Cybersecurity Requirements for Financial Institutions" published on September 19, 2016.

[1] 23 NYCRR § 500.

© Cleary Gottlieb Steen & Hamilton LLP, 2017. All rights reserved.
This memorandum was prepared as a service to clients and other friends of Cleary Gottlieb to report on recent developments that may be of interest to them. The information in it is therefore general, and should not be considered or relied on as legal advice. Throughout this memorandum, "Cleary Gottlieb" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions, and the term "offices" includes offices of those affiliated entities.

KEY CHANGES FROM INITIAL DRAFT

Following the publication of the initial proposed regulations on September 13, 2016, the DFS received over 150 comments, many of them criticizing the proposed regulations for being overly prescriptive and insufficiently tied to the results of the risk assessment required to be conducted by the Covered Entity. In response, the DFS published revised proposed regulations on December 28, 2016 which showed movement toward greater flexibility and individualization and reflected a more risk-adjusted approach. The final Regulations were posted to the State Register on February 16, 2017.

In the final Regulations, the entire cybersecurity program as well as the applicability and implementation of certain specific security measures (including penetration testing and vulnerability assessments, use of multi-factor authentication and encryption of non-public information) are explicitly contextualized by (*i.e.*, the need to comply with them depends on) the risk assessment conducted by the Covered Entity. In addition, other requirements were softened by including materiality qualifiers (such as in the notice to superintendent requirement) and reducing the minimum frequency of certain requirements from annual to periodic.

Furthermore, in response to concerns about confidentiality, under the final Regulations any information provided by a Covered Entity pursuant to the Regulations is exempt from disclosure under other state or federal law.

However, the final Regulations are more onerous than the initial proposal in one significant regard, specifically with respect to documentation obligations. While the Regulations principally act to codify the existing practices of sophisticated institutions, Covered Entities must now maintain evidence comprehensively documenting such practices (including all records, schedules and data supporting the certificate of compliance for five years) and make such documentation available to the DFS upon request.

KEY TERMS

The Regulations are broader than the GLBA in two important respects, described below.

Covered Entities

The GLBA and the Regulations significantly overlap but are not entirely co-extensive in terms of applicability. The GLBA applies to "financial institutions," defined as any institution significantly engaged in financial activities, such as lending, insuring or providing investment services. By contrast, the Regulations apply to any non-governmental entity operating under a "certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Laws," which could encompass an extremely broad range of businesses given the vast scope of New York banking, insurance, and financial services laws.

Nonpublic Information

Under the Regulations, the scope of the definition of Nonpublic Information is significantly broader than under the GLBA.

The information protected by the GLBA is limited to personally identifiable financial information, whereas the definition of **Nonpublic Information** protected under the Regulations encompasses all nonpublic electronic information, even if not personally identifiable or financial information, that is (1) business-related information "the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity," (2) concerning an individual which, because of an identifier such as a name or number, could be used to identify such individual in combination with other data, such as a social security number, driver's license, financial account information, or biometric records or (3) created by or derived from a health care provider or an individual and related to the health or condition of any individual or family member (except age or gender).

The expanded definition of Nonpublic Information appears to reflect the Regulations' broader scope, intended to address cybersecurity risks generally, whether or not related to privacy.

KEY REQUIREMENTS

If the entity and the information are covered, the Regulations include new requirements that have

not previously been included in the GLBA, described below.

Personnel

Each Covered Entity must designate a qualified individual to act as a chief information security officer (**CISO**), responsible for developing and presenting a written report to the board of directors on at least an annual basis. The report must cover the Covered Entity's cybersecurity program and material cybersecurity risks. Unlike the initial proposed regulations which required the CISO to be employed by the Covered Entity, the final Regulations allow for the CISO to be employed by an affiliate or a third party service provider.

In addition, each Covered Entity must utilize qualified cybersecurity personnel sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the core cybersecurity functions.[2]

Reporting obligations

A Covered Entity must notify the DFS of any act or attempt to gain unauthorized access to, or to disrupt or misuse, its information system or information stored on such system (such act or attempt, a **Cybersecurity Event**) that (i) triggers a notice requirement with respect to a government body, self-regulatory agency or any other supervisory body or (ii) has a reasonable likelihood of materially harming a material part of normal operations. The notification to the DFS must occur within 72 hours after the Covered Entity determines that such an event has occurred.

Furthermore, beginning February 15, 2018, the chairperson of the board of directors of each Covered Entity must submit on an annual basis a signed certification stating that, to the best of the board of director's knowledge, their institution's cybersecurity program complies with the Regulations.

While the Regulations are silent with regards to the penalties for filing a false or incorrect certification, a certifying officer whose Covered Entity is subsequently found to be non-compliant could potentially incur personal civil liability.

Documentation obligations

Each Covered Entity must make all documentation and information relevant to its cybersecurity program available to the DFS upon request, including but not limited to the following: (1) written cybersecurity policy, (2) annual CISO report to board of directors, (3) documentation of cybersecurity monitoring and testing (including penetration testing and vulnerability assessments), (4) records for its systems designed to reconstruct material transactions and audit trails, (5) written procedures, guidelines and standards relating to application security, risk assessment and third party service provider security, (6) written incident response plan, (7) annual certification of compliance (and all records, schedules and data supporting the certificate for a period of five years) and (8) documentation of all areas, systems or processes that require material improvement, updating or redesign, and the remedial efforts planned and underway to address such deficiencies.

Third party service providers

Each Covered Entity must implement written policies and procedures addressing security concerns associated with third parties who provide services to the Covered Entity and maintain, process or otherwise have access to its Nonpublic Information through the provision of such services. These policies must include, to the extent applicable, identification and risk assessment of third party service providers, minimum cybersecurity practices required to be met by such third party service providers, due diligence processes to evaluate the adequacy of such third party service providers' cybersecurity practices and periodic assessment of such third party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

[2] Under the Regulations, each Covered Entity's cybersecurity program must perform the following six "core" functions: (1) identify and assess cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's information systems, (2) use defensive infrastructure and implement policies and procedures to protect information systems and Nonpublic Information from unauthorized access, disruption and misuse, (3) detect attempts at unauthorized access, disruption or misuse, (4) respond to such attempts to mitigate any negative effects, (5) recover from such events and restore normal operations and service and (6) fulfill regulatory reporting obligations.

These policies and procedures must also contain relevant guidelines for due diligence or contractual protections relating to third party service providers, including those addressing: (1) the third party service provider's policies and procedures for access controls, (2) the third party service provider's policies and procedures for use of encryption, (3) notice from the third party provider of a Cybersecurity Event directly impacting the Covered Entity's information systems or Nonpublic Information being held by the third party service provider and (4) representations and warranties addressing the third party service provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's information systems or Nonpublic Information.

LIMITED EXCEPTIONS

Covered Entities with (1) fewer than 10 employees, including independent contractors, of the Covered Entity or its affiliates located in New York or responsible for the business of the Covered Entity, (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations, or (3) less than $10,000,000 in year-end total assets (including the assets of its affiliates) qualify for an exemption from certain of the requirements under the Regulations. However, such Covered Entities must still establish and maintain a cybersecurity program and a written cybersecurity policy (including with respect to third parties), limit access privileges, conduct a periodic risk assessment of information systems, limit data retention and report any Cybersecurity Events discussed above under "Reporting obligations" to the DFS within 72 hours.

Covered Entities that (a) do not control, access, generate or possess Nonpublic information other than information relating to their affiliates and are subject to Article 70 of New York insurance law or (b) do not operate, maintain, or use any information systems and do not control, access, generate or possess Nonpublic Information qualify for an exemption from the majority of the requirements under the Regulations; however, such Covered Entities must still conduct periodic risk assessments, implement third party service provider security policies and limit data retention.

A Covered Entity must file a notice of exemption within 30 days of determining that it is exempt.

TRANSITION PERIODS

The Regulations entered into effect on March 1, 2017, and Covered Entities generally have 180 days from such date in which to comply with most requirements. However, Covered Entities will have additional transitional periods to comply with certain provisions, specifically: (a) one year to comply with the requirements relating to (i) the CISO's first written report, (ii) penetration testing and vulnerability assessments, (iii) risk assessment, (iv) multi-factor authentication and (v) cybersecurity awareness training for all personnel, (b) 18 months to comply with the requirements relating to (i) audit trails, (ii) application security, (iii) limitations on data retention, (iv) monitoring the activity of authorized users and (v) encryption of nonpublic information and (c) two years to comply with the requirements relating to third party service provider security policies.

CONCLUSION

The Regulations highlight the ongoing shift in public policy towards a more careful and regulated approach with respect to data privacy and serve as a timely reminder of the importance of continually assessing and managing risk in an environment of escalating cybersecurity threats. In this context, it is important to bear in mind that other legislative measures addressing cyber risks are expected to be adopted at both the state and federal level, including the proposal from the Board of Governors of the Federal Reserve Systems, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation for rules regarding enhanced cyber risk management standards for certain entities under such agencies' supervision (mainly large financial institutions). For entities subject to both the Regulations and such other legislative measures, compliance with the various requirements and standards may become complicated and costly so it is hoped that these other measures will be largely consistent with the Regulations.

…

CLEARY GOTTLIEB