ALERT MEMORANDUM - SEPTEMBER 20, 2016

LEGAL UPDATE

New York Regulators Propose Cybersecurity Requirements for Financial Institutions

The recently proposed New York cybersecurity regulations set forth some new and notable reporting requirements but are otherwise duplicative of certain federal requirements applicable to financial institutions and codify the existing practices of sophisticated institutions.

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

Giovanni Prezioso
T: +1 202 974 1650
gprezioso@cgsh.com

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

The full text of the proposed regulations can be accessed via this link: *http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf*

OVERVIEW

On September 13, 2016, the New York Department of Financial Services (**DFS**) issued proposed cybersecurity regulations for public comment.[1] Under the proposed regulations, any individual, partnership, corporation, 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**) will be required to assess their cybersecurity risks and establish and maintain a cybersecurity program designed to address such risks in a "robust" fashion. The regulations will be open for public comment for 45 days, unless extended.

The regulations are a direct response to the increasing number of cyber-attacks on financial institutions and insurers, such as the 2014 cyber-attack on JPMorgan Chase in which 83 million accounts were compromised and the 2015 cyber-attack on Anthem, Inc. in which 78 million unencrypted records containing personal information were stolen.

These regulations represent the first comprehensive state regulatory proposal to address cybersecurity. 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, including banks, securities firms and insurance companies. For example, the proposed regulations essentially duplicate the mandates under the GLBA that require Covered Entities to develop a written information security plan for protecting non-public customer information, employ data encryption, implement access controls, conduct regular testing of their security programs and design an incident response plan.

However, some requirements of the proposed regulations will constitute entirely new obligations, such as designating a chief information security officer, submitting a written statement of compliance on an annual basis and reporting any unauthorized access attempts to the DFS within 72 hours.

[1] 23 NYCRR § 500.

KEY TERMS

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

Covered Entities

The GLBA and the proposed 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 proposed regulations will apply to any entity operating under a "certificate, permit, accreditation or similar authorization under banking, insurance or 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.

The concept of "similar authorization" is particularly broad. For example, it could cover any type of independent contractor of a larger company who is required to obtain a license in New York and has more than 1,000 customers. This expansiveness is only partially ameliorated by the limited exception for smaller entities discussed below.

Nonpublic Information

Under the proposed 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 proposed regulations will encompass all nonpublic electronic information, even if it is not personally identifiable or financial information. The proposed regulations protect information if it 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) obtained by a Covered Entity about an individual in connection with providing a financial product or service to such individual, or (3) created by, derived or obtained from a health care provider or an individual and relates to the health or condition of any individual or family member (except age or gender). The proposed definition of Nonpublic Information also includes personally identifiable financial information, namely "information that can be used to distinguish or trace an individual's identity."

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 NEW REQUIREMENTS

If the entity and the information are covered, the proposed regulations include new requirements that have not previously been included in the GLBA, described below.

Personnel

Each Covered Entity must designate a chief information security officer, responsible for developing and presenting a report to the board of directors on at least a bi-annual basis. The report, which must be made available to the DFS, will assess the confidentiality and integrity of the Covered Entity's information systems, describe any exceptions to its cybersecurity policies and procedures, identify cyber risks, assess the effectiveness of the cybersecurity program, propose steps to remediate any inadequacies identified therein, and include a summary of all material cybersecurity events.

In lieu of appointing a chief information security officer, a Covered Entity may delegate the responsibility for overseeing and implementing a cybersecurity program and enforcing its cybersecurity policy to a third party service provider, provided that such Covered Entity designates a senior member of its personnel responsible for oversight of such third party provider.

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

[2] Under the regulations, each Covered Entity's cybersecurity program must perform the following six "core" functions: (1) identify cyber risks by, at a minimum,

employ a third party provider for such purposes. Please refer to the discussion of third party providers herein for information on the requirements with respect to such service providers.

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 has a reasonably likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information (including even the *potential* unauthorized tampering with, access to or use of Nonpublic Information), or any other material risk of imminent harm relating to its cybersecurity program. The notification to the DFS must occur within 72 hours after the Covered Entity becomes aware of such event.

Furthermore, beginning January 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. The certification must include a description of any material risks of imminent harm to the cybersecurity program identified by the Covered Entity in the preceding year.

While the proposed regulations are silent in 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.

Third party providers

Each Covered Entity must implement written policies and procedures addressing security concerns associated with third parties that have access to such Covered Entity's information systems and Nonpublic Information. These policies must include identification and risk assessment of third parties, establish minimum cybersecurity practices required to be met by such third parties, set forth due diligence processes to evaluate the adequacy of third party cybersecurity practices and provide for periodic assessment on at least an annual basis of such third parties and the continued adequacy of their cybersecurity practices.

These policies and procedures must also contain preferred provisions to be included in contracts between the Covered Entity and its third party service providers. Such provisions must address, to the extent applicable, (1) the use of multi-factor authentication, (2) the use of encryption, (3) prompt notice of a Cybersecurity Event affecting the third party service provider, (4) identity protection services to be provided for any customers materially impacted by a Cybersecurity Event resulting from the third party service provider's negligence or willful misconduct, (5) representations and warranties from the third party service provider that the service or product provided to the Covered Entity is free of viruses, trap doors, time bombs and other mechanisms that would impair the security of the Covered Entity's information systems or Nonpublic Information, and (6) the right of the Covered Entity to perform audits of the third party service provider's cybersecurity.

Limited exceptions

Covered Entities with (1) fewer than 1,000 customers in each of the last three calendar years, (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and (3) less than $10,000,000 in year-end total assets (including the assets of its affiliates) qualify for an exemption from some of the requirements, such as appointing a chief information security officer, employing cybersecurity personnel, conducting multi-factor authentication, encrypting Nonpublic Information and devising an incident response plan. However, such Covered Entities must still

identifying the Nonpublic Information stored on the Covered Entity's information systems, the sensitivity of such Nonpublic Information, and how and by whom such Nonpublic Information may be accessed, (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.

establish and maintain a cybersecurity program and a written cybersecurity policy (including with respect to third parties), limit access privileges, conduct a risk assessment of information systems on at least an annual basis, limit data retention and report any Cybersecurity Events to the DFS within 72 hours.

CONCLUSION

The regulations will become effective on January 1, 2017, and Covered Entities will have 180 days from such date in which to comply with the requirements.

The regulations will likely have the most significant impact on smaller, local banks and insurers that, unlike larger financial institutions that are already subject to the GLBA and devote immense resources to cybersecurity efforts, will now need to bring their cybersecurity programs up to the minimum standards established in the proposed regulations.

Nevertheless, the proposal highlights the ongoing shift in public policy towards a more careful and regulated approach with respect to data privacy and serves as a timely reminder of the importance of continually assessing and managing risk in an environment of escalating cybersecurity threats.

…

CLEARY GOTTLIEB