ALERT MEMORANDUM

NYDFS Cybersecurity Regulations Take Effect

August 21, 2017

I. Introduction

New York's new cybersecurity regulations (the "Regulations") become effective on August 28, 2017, marking a significant milestone in what is likely to be a new era in cybersecurity regulation on both a national and international level. As governments grapple with how best to address cyber threats to their citizens, businesses and national security, there is an increasing focus on the potential use of regulatory requirements to impose minimum cybersecurity standards, particularly in the financial services sector. As more states and nation states adopt cybersecurity requirements, financial institutions are facing increased compliance costs and potentially a diversion of resources away from risk mitigation to compliance with regulatory requirements. As this trend develops, key factors in managing the growing patchwork of requirements will be working to avoid overly prescriptive, highly specific requirements and trying to ensure a degree of harmonization, for example with the National Institute of Standards and Technology's Cybersecurity Framework. In the short term, financial firms will focus on identifying the applicable regulatory framework that sets the highest bar and building systems to comply that should generally provide for compliance globally. As of today, the Regulations are a key element of that high bar and already are playing a role in setting expectations for best practices across the industry. As the Regulations come into effect, we briefly take stock of their requirements and related global developments.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

NEW YORK

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

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

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

WASHINGTON

Katherine Mooney Carroll
+1 202 974 1584
kcarroll@cgsh.com

Michael H. Krimminger
+1 202 974 1720
mkrimmingger@cgsh.com

II. August 28, 2017 Requirements

Beginning on August 28, 2017, all individuals and companies 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 Entity") must:

1. develop a cybersecurity program,
2. develop a cybersecurity policy,
3. designate a Chief Information Security Officer ("CISO"),
4. limit who has access to data or systems,
5. use qualified cybersecurity personnel to manage cybersecurity risks,
6. notify the DFS[1] of a cybersecurity event within 72 hours, and
7. have a written incident response plan.[2]

The details of each of the aforementioned requirements are described below. Compliance with these requirements must be certified by a Senior Officer[3] or the board of directors of the Covered Entity by February 15, 2018.

1. **Cybersecurity Program**.[4] Each Covered Entity must establish and maintain a cybersecurity program, based on the Covered Entity's risk assessment, designed to protect the confidentiality, integrity and availability of the Covered Entity's information systems. Note that while Covered Entities are not required to complete the risk assessment until March 1, 2018, the cybersecurity program (and certain other requirements such as cybersecurity policy and access privileges) needs to be implemented this month so Covered Entities should consider completing a reasonable risk assessment by August 28, 2017 in order to demonstrate clear compliance with those other requirements. The compliance program must: (i) identify and assess internal and external cybersecurity risks; (ii) use defensive infrastructure to protect information systems and Nonpublic Information[5] stored on such systems; (iii) detect cybersecurity events (which include both successful and unsuccessful attempts to gain unauthorized access to, disrupt or misuse an Information System or information stored on it); (iv) respond to detected cybersecurity events to mitigate any negative effects; (v) recover from cybersecurity events and restore normal operations and services; and (vi) fulfill applicable regulatory reporting obligations.
2. **Cybersecurity Policy**.[6] Each Covered Entity must implement and maintain a cybersecurity policy based on the Covered Entity's risk assessment and approved by a Senior Officer or the board of directors. The Policy must address the following areas to the extent applicable to the Covered Entity's operations: (i) information security; (ii) data governance and classification; (iii) asset inventory and device management; (iv) access controls and

[1] *DFS* means the New York State Department of Financial Services.
[2] 23 NYCRR § 500.
[3] *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to the Regulations.
[4] 23 NYCRR § 500.002.
[5] *Nonpublic Information* shall mean all electronic information that is not publicly available information and (i) is Business related information of a Covered Entity 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; (ii) can be used to identify an individual, in combination with any additional identifying data elements, such as social security number, drivers' license number, account number, credit or debit card number; or (iii) is any health-related information or data, except age or gender.
[6] 23 NYCRR § 500.03.

identity management; (v) business continuity and disaster recovery planning and resources; (vi) systems operations and availability concerns; (vii) systems and network security; (viii) systems and network monitoring; (ix) systems and application development and quality assurance; (x) physical security and environmental controls; (xi) customer data privacy; (xii) vendor and Third Party Service Provider[7] management; (xiii) risk assessment; and (xiv) incident response.

3. **Chief Information Security Officer**.[8] Each Covered Entity must designate a qualified individual to oversee and implement the cybersecurity program and enforce the cybersecurity policy (i.e., a Chief Information Security Officer or CISO). If the CISO is a Third Party Service Provider, the Covered Entity retains responsibility for compliance and must (i) designate a senior personnel member to direct and oversee the Third Party Service Provider and (ii) require the Third Party Service Provider to maintain a cybersecurity program. Beginning March 2018, the CISO will also have to submit a written report on the cybersecurity program and material cybersecurity risks at least annually to the board of directors or equivalent governing body.

4. **Access Privileges**.[9] Based on the Covered Entity's risk assessment, each Covered Entity must limit user access privileges to information systems that provide access to Nonpublic Information and must periodically review such access privileges.

5. **Cybersecurity Personnel and Intelligence**.[10] Each Covered Entity must utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider that will: (i) manage cybersecurity risks and (ii) perform or oversee the performance of core cybersecurity functions. The Covered Entity must provide the cybersecurity personnel with cybersecurity updates and training.

6. **Incident Response Plan**.[11] Each Covered Entity must have a written incident response plan that is designed to promptly respond to, and enable recovery from, any material cybersecurity event and addresses: (i) internal processes for responding to a cybersecurity event; (ii) the goals of the incident response plan; (iii) the definition of clear roles, responsibilities and levels of decision-making authority; (iv) external and internal communications and information sharing; (v) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; (vi) documentation and reporting regarding cybersecurity events and related incident response activities; and (vii) the evaluation and revision as necessary of the incident response plan following a cybersecurity event.

7. **Notices to Superintendent**.[12] Each Covered Entity must notify NY's Superintendent of Financial Services within 72 hours of a cybersecurity event that either (i) impacts the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (ii) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

[7] *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

[8] 23 NYCRR § 500.04.
[9] 23 NYCRR § 500.07.
[10] 23 NYCRR § 500.10.
[11] 23 NYCRR § 500.16.
[12] 23 NYCRR § 500.17.

These requirements will likely have the most significant impact on smaller, local banks and insurers that, unlike larger financial institutions that are already subject to the Gramm-Leach-Bliley Act and devote immense resources to cybersecurity efforts, will now need to bring their cybersecurity programs up to the minimum standards established in the Regulations.[13]

III. Other Key Deadlines

Covered Entities will have additional transitional periods to comply with certain provisions, specifically: (i) until March 1, 2018 to comply with the requirements relating to the CISO's first written report, penetration testing and vulnerability assessments, risk assessment, multi-factor authentication and cybersecurity awareness training, (ii) until September 1, 2018 to comply with the requirements relating to audit trails, application security, limitations on data retention, monitoring the activity of authorized users and encryption and (iii) until March 1, 2019 to comply with the requirements relating to third-party service provider security policies.

IV. Exceptions to Compliance

Covered Entities qualify for an exemption from certain of the requirements under the Regulations if (i) fewer than 10 employees, including independent contractors, of the Covered Entity or its affiliates are located in New York or responsible for the business of the Covered Entity, (ii) they had less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations or (iii) they had less than $10,000,000 in year-end total assets (including the assets of its affiliates). With respect to the August 28, 2017 requirements, such entities are not mandated to appoint a CISO, utilize qualified cybersecurity personnel or have a written incident response plan. 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 and report any cybersecurity events to the Superintendent within 72 hours.

Covered Entities also qualify for an exemption from the majority of the requirements under the Regulations if they (i) 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 (ii) do not operate, maintain or use any information systems and do not control, access, generate or possess Nonpublic Information. A Covered Entity must file a notice of exemption within 30 days of determining that it is exempt.

V. The Patchwork of Regulations

In addition to the New York Regulations, there is a patchwork of rules that also could apply to entities in other jurisdictions, and large institutions operating in multiple jurisdictions must ensure compliance across multiple regulatory regimes. For example:

United States. While New York's Regulations were the first of its kind in the United States, other U.S. states are likely to follow. Colorado recently passed cybersecurity rules for broker-dealers and investment advisers subject to the Colorado Securities Act. Although the Colorado rules contain requirements similar to those in the Regulations, such as the requirements that entities conduct an annual cybersecurity risk assessment and implement and maintain cybersecurity procedures to address access controls and use of encryption, the Colorado regulations also contain some unique instructions. For example, to the extent possible, a firm's cybersecurity procedures must contain procedures for authenticating client instructions received via electronic communication.

There have also been cybersecurity initiatives at the federal level. In October 2016, three federal banking regulators[14] put forward a joint advance notice for "Enhanced Cyber Risk Management Standards" to apply to large entities in the financial sector. The

[13] https://www.clearygottlieb.com/news-and-insights/publication-listing/new-york-proposes-first-of-its-kind-cybersecurity-regulation

[14] The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation.

public comment period for the proposal expired January 17, 2017. On August 7, 2013, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") published a list of robust policies and procedures that firms "may wish to consider" implementing based on the results of the OCIE's second cybersecurity survey of 75 registered broker-dealers, investment advisers and investment companies.[15]

International. Outside of U.S. borders, the EU and China, among others, have enacted comprehensive cybersecurity regulations. Most significantly, in the EU, organizations established or providing services in the EU will be subject to new national and EU-wide cybersecurity legislation through the General Data Protection Regulation and national legislation implementing the Network and Information Security Director. These requirements come into effect in May 2018; the scope and key terms of such regulations are discussed in our alert memorandum "Cybersecurity in the EU – The New Regime under the GDPR and NISD" published May 3, 2017.[16] A number of other sector-specific laws impose similar cybersecurity obligations on organizations operating in the payment services and electronic trust services sectors.[17]

Additionally, China's *PRC Network Security* Law went into effect June 1, 2017. It requires broadly defined "network operators" to protect the security of personal data. Network operators, among other requirements, are obligated to carry out a risk assessment at least annually and file a report to the relevant Chinese governmental agencies. In addition, organizations that operate "critical information infrastructure" are subject to additional requirements in respect of the storage and transfer of personal information and "important data" collected or generated within China, including obligations to store in-scope information and data within China and observe stringent restrictions on data export including, in certain circumstances, submitting to a security assessment by a Chinese regulator.

VI. Key Takeaways

The Regulations reflect a growing global concern for promoting cybersecurity and protecting personal data.

Within the United States, we expect that more states will follow the lead of New York and Colorado in passing their own cybersecurity rules. Coupled with potential federal regulations for financial institutions, these legislative measures would collectively create a complex web of regulations for entities that operate across state borders. Entities will need to expend considerable resources to determine which rules cover their operations and to ensure compliance with the substantive and reporting obligations. The best possible outcome of the likely expansion of these rules to other U.S. jurisdictions, given the breadth of the cybersecurity measures adopted or proposed thus far, is that they will be similar in all materials respects to the Regulations, and that the federal regulations will include high-level guidance or broad standards rather than specific prescriptive requirements (unless these are consistent with the Regulations). Such consistency (and, possibly, a certain level of harmonization) will make compliance less burdensome on regulated entities and pertinent third-party service providers that serve such regulated entities. (Of course, if the state-by-state data breach notification laws are any guide, each jurisdiction is likely to impose its own specific set of rules that often differ in substantial ways from each other). Moreover, we can safely assume that additional measures will be adopted in the coming months in other non-U.S. jurisdictions as well.[18]

[15] *See* https://www.clearygottlieb.com/news-and-insights/publication-listing/sec-issues-risk-alert-based-on-cybersecurity-survey-8-11-17.

[16] https://www.clearygottlieb.com/news-and-insights/publication-listing/cybersecurity-in-the-eu-the-new-regime-under-the-gdpr-and-nisd-5-5-17.

[17] Directive (EU) 2015/2366 (Payment Services 2 Directive) and Regulation (EU) 2014/910 (Electronic Identification Regulation).

[18] *See, e.g.*,https://www.clearygottlieb.com/news-and-insights/publication-listing/sec-issues-risk-alert-based-on-cybersecurity-survey-8-11-17; https://www.clearygottlieb.com/news-and-

Finally, it is important to bear in mind that despite the costs associated with complying with an array of regulations, the various rules create a benchmark for proper cybersecurity practices. Cyber-attacks and personal data loss present substantial risks to the operations for all entities, and the likelihood of follow-on civil and regulatory litigation is substantial.[19] As such, at a minimum, all organizations, even organizations not subject to any of the aforementioned regulations, should consider any cybersecurity rules and standards as indicators of what may be considered best practices; adopting a cybersecurity program consistent with these requirements can help reduce that regulatory and civil litigation exposure, while also protecting the operations and reputation of the business.

…

CLEARY GOTTLIEB

insights/publication-listing/mitigating-litigation-and-regulatory-exposure-from-cyber-attacks.

[19] *See* https://www.clearygottlieb.com/news-and-insights/publication-listing/mitigating-litigation-and-regulatory-exposure-from-cyber-attacks.