MAYER·BROWN

Legal Update
March 21, 2017

Cybersecurity: NY Adopts Final Regulations for Banks, Insurance Businesses and Other Financial Services Institutions

On February 16, 2017, the New York State Department of Financial Services ("NYDFS") finalized regulations that mandate cybersecurity standards for all institutions authorized by NYDFS to operate in New York, including many banks, insurance entities and insurance professionals doing business in New York.[1] The final regulations, titled "Cybersecurity Requirements for Financial Services Companies" ("Final Regulations"), implement a significantly revised version of the NYDFS's September 13, 2016, proposal. (*See* our **September 22, 2016, Legal Update** for an analysis of the original proposal.) The Final Regulations became effective on March 1, 2017 ("Effective Date"), but there is a phase-in period as described below. In addition, the NYDFS issued frequently asked questions with corresponding answers on March 13, 2017 (the "FAQs").[2]

The intent of the Final Regulations is to "require effective cybersecurity to protect consumers" and NYDFS-regulated institutions. Acknowledging that the "number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark," the Final Regulations explicitly state that cybersecurity is a "priority for New York State."

The Final Regulations are quite comprehensive and address everything from access controls and encryption to data disposal and employee training. We expect they will have significant ramifications not only for large institutions but also many medium-sized institutions that have only limited operations in New York and are already staggering under the post-financial crisis regulatory burden. Despite expanded exemptions, the Final Regulations will cover many small institutions and impose significant new compliance costs.

This Legal Update (i) describes the relevant definitions and institutions affected by the Final Regulations, (ii) explains their substantive requirements and (iii) highlights some of the takeaways for the financial services industry.

I. Definitions and Scope

Covered Entity: The Final Regulations apply to any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York Banking, Insurance, or Financial Services Laws. This definition is intended to be broad, and indeed, many institutions are evaluating if they fall within the scope of the Final Regulations.

On the banking side, although it is clear that banks and trust companies that are formed under New York law are within the scope of the Final Regulations, it remains to be seen how NYDFS will apply the Final Regulations to institutions that have no physical presence in New York (e.g., non-New York banks that are registered as exempt mortgage servicers), institutions with minimal operations (e.g., loan production offices) and non-New York

institutions whose New York presence is not operationally separate (e.g., non-New York state banks that have domestic branches registered with NYDFS).

Additionally, the FAQs confirm that non-US institutions will need to apply the rule to Covered Entities that are technically registered or authorized by NYDFS but may not have their own information systems or possess customer data that is segregated from their home offices (e.g., New York branches, agencies and representative offices of non-US banks). The FAQs indicate that such a Covered Entity should apply the Final Regulations only to information systems that support its operations and Nonpublic Information (defined below) that belongs to it.

On the insurance side, Covered Entities include not only insurance companies (regardless of domicile) that are licensed to do business in New York but also other types of business entities *and individual professionals* (again, regardless of domicile) that are licensed under the New York Insurance Law, such as insurance agents and brokers, insurance adjusters and reinsurance intermediaries.

Nonpublic Information: Nonpublic Information is defined as any electronic information that is not publicly available and that is (i) business-related information, the unauthorized disclosure or destruction of which would cause a material adverse impact on the Covered Entity; (ii) information concerning an individual that could be combined with specified data elements to identify the individual; or (iii) derived from an individual or healthcare provider and related to certain healthcare information (except for age and gender).

Cybersecurity Event: Cybersecurity Event is defined as any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such a system.

Third Party Service Provider: Third Party Service Provider ("TSP") is defined as any 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.

II. Substantive Requirements

A Covered Entity is expected to maintain a written cybersecurity policy or policies and implement a risk-based cybersecurity program. A Covered Entity must also satisfy specific requirements related to (i) risk assessment, (ii) personnel, (iii) application security, (iv) access privileges, (v) Cybersecurity Event notification, (vi) multi-factor authentication, (vii) encryption, (viii) audit trail, (ix) data disposal, (x) TSPs and (xi) reporting to NYDFS. The Final Regulations provide phase-in periods for certain requirements and exemptions for certain Covered Entities.

Cybersecurity Policy and Program.
A Covered Entity is required to maintain a cybersecurity program that is based on its risk assessment (discussed below) and designed to identify and assess cybersecurity risks; protect information systems and Nonpublic Information; detect, mitigate and recover from Cybersecurity Events; and fulfill applicable regulatory reporting obligations.

A Covered Entity is required to implement its cybersecurity program through written policies and procedures that are based on its risk assessment, and such policies and procedures should be approved by a senior officer or the board of directors (or equivalent body). To the extent applicable, such policies and procedures should address:

- Information security;
- Data governance and classification;
- Asset inventory and device management;

- Access controls and identity management;
- Business continuity and disaster recovery planning and resources;
- Systems operations and availability concerns;
- Systems and network security;
- Systems and network monitoring;
- Systems and application development and quality assurance;
- Physical security and environmental controls;
- Customer data privacy;
- Vendor and TSP management;
- Risk assessment; and
- Incident response.

Risk Assessment and Testing Requirements. A Covered Entity must conduct a periodic risk assessment of its information systems to inform its cybersecurity program. The risk assessment should reflect changes in controls and technology, as well as evolving threats and cybersecurity risks to the Covered Entity. The risk assessment must be documented and should be conducted in accordance with written policies and procedures and include specifications for how the Covered Entity will accept or mitigate identified risks.

To the extent it does not engage in effective continuous monitoring, or use other systems to identify vulnerabilities, a Covered Entity is required to conduct annual risk-based penetration testing and biennial vulnerability assessments to gauge the effectiveness of its cybersecurity program. In the FAQs, the NYDFS clarified that continuous monitoring means that the Covered Entity "has the ability to continuously, on an ongoing basis, detect changes or activities within a Covered Entity's Information Systems that may create or indicate the existence of cybersecurity vulnerabilities or malicious activity." Manual log review and firewall configurations would not qualify under this definition.

Chief Information Security Officer and Personnel. A Covered Entity must designate a Chief Information Security Officer ("CISO"), who should be responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its policy. At least annually, the CISO must provide a report to the Covered Entity's board or other governing body on the cybersecurity program and material cybersecurity risks, considering, as applicable, features including material Cybersecurity Events and the overall effectiveness of the program. Certain CISO functions may be outsourced to an affiliate or TSP, but a Covered Entity nevertheless remains responsible for complying with the Final Regulations.

A Covered Entity is required to employ cybersecurity personnel sufficient to maintain and execute the Covered Entity's cybersecurity program. The cybersecurity personnel must be subject to ongoing subject-matter training requirements, and all of a Covered Entity's personnel must undergo regular cybersecurity awareness training that is updated to reflect risks identified in its periodic risk assessment (discussed above). The Covered Entity also must implement risk-based controls to monitor the activities of authorized personnel to detect unauthorized access or use of Nonpublic Information.

Application Security. A Covered Entity must implement and comply with written procedures and standards for the secure development of in-house applications and testing of externally developed applications. These written materials must be periodically reviewed, assessed and updated by the CISO or a qualified designee.

Access Privileges and Identity Management. Covered Entities are required to periodically review the access privilege of authorized users of its systems, as well as limit access privileges as appropriate, based on their risk assessment.

Incident Reporting and Cybersecurity Event Notification. A Covered Entity must

put in place a written incident response plan designed to enable the entity to promptly respond to and recover from a Cybersecurity Event materially affecting the confidentiality, integrity or availability of its systems. The Final Regulations specifically require an incident response plan to address seven areas:

- Internal processes for responding to a Cybersecurity Event;
- Goals of the incident response plan;
- Clearly defined roles, responsibilities and levels of decision-making authority;
- External and internal communications plans and information sharing;
- Identification of requirements for the remediation of identified weaknesses;
- Documentation and reporting of Cybersecurity Events and related incident response activities; and
- Evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Additionally, Covered Entities are required to notify NYDFS within 72 hours after becoming aware of any Cybersecurity Event with a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" or for which notice must be provided to any government body, self-regulatory agency or other supervisory body.

Multi-factor Authentication. The Final Regulations mandate the use of multi-factor authentication methods (e.g., password and token or text messaging code) for individuals accessing the Covered Entity's internal systems from an external network unless the CISO has approved the use of an equivalent or more secure alternative. The Final Regulations also require the use of effective controls, which may include multi-factor or risk-based authentication (requiring additional verification, such as the use of challenge questions, when anomalies or changes in normal use patterns of a user are detected) in other situations, based on the Covered Entity's risk assessment.

Data Encryption. Based on its risk assessment, a Covered Entity will need to encrypt Nonpublic Information that it stores or transmits over external networks, though the Final Regulations provide that where encryption is currently infeasible, appropriate alternative compensating controls may be reviewed and approved by the CISO so long as they are re-reviewed at least annually.

Audit Trail. A Covered Entity must, based on its risk assessment, maintain (i) its systems so that it is able to reconstruct material financial transactions to support normal operations and (ii) audit trails that are designed to detect and respond to Cybersecurity Events that present a material risk to the Covered Entity. These transaction records must be maintained for at least five years, and the audit trail records must be maintained for at least three years.

Data Disposal. A Covered Entity must have policies and procedures for the secure disposal of Nonpublic Information that is no longer necessary for its business, except where retention is required by another law or regulation.

Third Party Service Providers. The use of TSPs as a potential point of access for unauthorized parties continues to be a particular area of concern for NYDFS and other regulators. The Final Regulations, therefore, overlay on TSPs most of the provisions applicable to Covered Entities by directing Covered Entities to develop written policies and procedures designed to ensure security of systems and data accessible to, or held by, TSPs.

Covered Entities are expected to perform a risk assessment on their TSPs and conduct due diligence on, and periodic risk-based assessments of, their TSPs' cybersecurity practices. TSPs would be required to meet minimum cybersecurity standards (defined by the Covered Entities) in order to do business

with Covered Entities. Additionally, each Covered Entity would be required to establish "preferred provisions" for service contracts with their TSPs addressing (i) the use of access controls and multi-factor authentication, (ii) encryption of Nonpublic Information in transit and at rest, (iii) prompt notification to the Covered Entity of certain Cybersecurity Events and (iv) representations and warranties from the TSPs concerning the policies and procedures that relate to the security of the Covered Entity's systems or Nonpublic Information.

Annual Certification. The chairperson of the board of directors (or a senior officer) of the Covered Entity is required to sign an annual certification to NYDFS, stating that to the best of the certifying individual's knowledge, the Covered Entity is in compliance with the Final Regulations. The certification is due by February 15 of each year beginning in 2018. A Covered Entity is required to maintain the documentation supporting its certification for a period of five years, and that documentation must be available for inspection by NYDFS. To the extent a Covered Entity has identified areas that require improvement, updating or redesign, the documentation needs to address those areas and the remedial efforts that are underway or planned.

Phase-in Period. A Covered Entity must generally comply with the Final Regulations as of August 28, 2017 (180 days after the Effective Date). A Covered Entity, however, is not required to comply with:

1. (i) CISO reporting, (ii) penetration testing, (iii) vulnerability assessment, (iv) risk assessment, (v) multi-factor authentication and (vi) enterprise-wise cybersecurity awareness training until March 1, 2018;
2. (i) audit trail, (ii) application security, (iii) data disposal, (iv) employee monitoring and (v) encryption requirements until September 3, 2018; and
3. The TSP requirements until March 1, 2019.

Exemptions. A Covered Entity that, when aggregated with its affiliates, has (i) fewer than ten New York employees, (ii) less than $5 million in New York revenue or (iii) less than $10 million in total assets is required to satisfy only the (1) cybersecurity policy and program, (2) access privileges, (3) risk assessment, (4) TSP, (5) data disposal and (6) NYDFS notice and reporting requirements. Individuals who are associated with a Covered Entity do not need to develop their own cybersecurity program if they are covered by the cybersecurity program of the Covered Entity with which they are associated. A Covered Entity that does not have information systems nor control or use Nonpublic Information is required to satisfy only the (1) risk assessment, (2) TSP, (3) record retention, and (4) NYDFS notice and reporting requirements. A Covered Entity must file a notice with NYDFS by September 27, 2017, to rely on any of the foregoing full or partial exemptions from the Final Regulations.[3] Certain specialized insurance institutions (i.e., charitable annuity societies, non-New York risk retention groups, and accredited and certified reinsurers) are exempt from the Final Regulations.

III. Takeaways

As noted in our **September 22, 2016, Legal Update**, the Final Regulations will affect financial institutions in a number of industries, including insurance, banking, consumer lending and money transmission. Although the Final Regulations are less prescriptive than the earlier proposals, they still impose significant requirements on Covered Entities and will require particular attention over the next few months to ensure compliance by August 28, 2017.

Covered Entities that operate in multiple states or that are part of integrated financial groups should assess their operations to determine which legal entities, systems and TSPs are in-scope. In addition, Covered Entities should review their existing policies and procedures to identify and remediate any gaps with the

requirements set forth in the Final Regulations. Failure to take these actions may present issues when the NYDFS conducts its next examination or the Covered Entity is required to certify its compliance with the Final Regulations in February 2018.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

Jeffrey P. Taft
+1 202 263 3293
jtaft@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

James R. Woods
+1 212 506 2390
jrwoods@mayerbrown.com

Lawrence R. Hamilton
+1 312 701 7055
lhamilton@mayerbrown.com

Steven M. Kaplan
+1 202 263 3005
skaplan@mayerbrown.com

Thomas J. Delaney
+1 202 263 3216
tdelaney@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

David L. Beam
+1 202 263 3375
dbeam@mayerbrown.com

David A. Tallman
+1 713 238 2696
dtallman@mayerbrown.com

Matthew Bisanz
+1 202 263 3434
mbisanz@mayerbrown.com

Endnotes

[1] NYDFS, *Press Release* (Feb. 16, 2017); *Cybersecurity Requirements for Financial Services Companies*, XXXIX (No. 9) N.Y. Reg. 3 (Mar. 1, 2017) (*codified at* N.Y. Comp. Codes R. & Regs. tit. 23, pt. 500).

[2] NYDFS, *Frequently Asked Questions Regarding 23 NYCRR Part 500* (Mar. 13, 2017).

[3] NYDFS, *Key Dates under New York's Cybersecurity Regulation (23 NYCRR Part 500)* (Mar. 16, 2017).