New York Department of Financial Services Cybersecurity Regulation Compliance and Certification Deadlines

New York Department of Financial Services ("DFS") Regulation 23 NYCRR 500 requires that entities regulated by the DFS comply[1] with the following requirements by certain deadlines, and that a senior officer or the board chairperson certify[2] compliance with the regulations by certain deadlines.

Comply by August 28, 2017 / Certify by February 15, 2018

Summary

By August 28, 2017, your company must be in compliance with the measures listed below and by February 15, 2018, a senior officer or the board of directors of your company must certify that your company is in compliance with those measures. Specifically, this signed certification would require that your company:

- Be able to notify the Superintendent of Financial Services ("Superintendent") within 72 hours of a Cybersecurity Event[3], which also requires your company to be able to assess its regulatory notification obligations within 72 hours of a Cybersecurity Event

[1] Under 500.19(a), covered entities with fewer than ten employees, less than $5,000,000 in gross annual revenue, or less than $10,000,000 in year-end total assets are exempt from the following DFS regulations: 500.04, 500.05, 500.06, 500.10, 500.12, 500.14, 500.15, and 500.16. Under 500.19(b), employees, agents, representatives, or designees of covered entities who are themselves covered entities are exempt. Under 500.19(c)-(d), covered entities that do not operate, maintain, utilize or control any Information Systems and are not required to work with Nonpublic Information and covered entities under Article 70 of the Insurance Law that are not required to work with Nonpublic Information are exempt from the following DFS regulations: 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16. Those covered entities qualifying for the above exemptions must file a Notice of Exemption within thirty days of determining covered entity is exempt. Under 500.19(f), persons subject to Insurance Law section 1110 or 5904, or any accredited reinsurer are exempt. If, at the end of a covered entity's fiscal year, it no longer qualifies for exemption, the covered entity must comply by 180 days after the end of its fiscal year.

[2] This certification should be based on the form in Appendix A.

[3] This and other defined terms are addressed in Appendix B.

- Designate a Chief Information Security Officer ("CISO")
- Implement an overall cybersecurity program
- Implement appropriate cybersecurity policies
- Develop an incident response plan
- Regulate access privileges for Information Systems
- Utilize and integrate qualified cybersecurity personnel

Descriptions of Relevant Measures

1. Notices to Superintendent of Financial Services ("Superintendent") [500.17]: Your company is prepared to:

☐ Notify the Superintendent of any Cybersecurity Event that:

- Requires notice to be provided to any of the following:
  - Government body
  - Self-regulatory agency
  - Other supervisory body; or
- Created a reasonable likelihood of materially harming any part of the normal operation of your company

☐ Submit such notice to the superintendent as promptly as possible, but in all cases within 72 hours of a determination that a relevant Cybersecurity Event has occurred

2. Chief Information Security Officer ("CISO") [500.04(a)]: A CISO

☐ Has been designated by your company

☐ Is qualified to oversee, implement, and enforce your company's cybersecurity program

- If the CISO is a third party service provider or an affiliate:
  - ☐ Your company is still able to certify compliance, as it retains responsibility for compliance
  - ☐ Your company has designated a senior personnel member to direct and oversee the third party service provider

☐ Your company requires the third party service provider to maintain a cybersecurity program

3. Cybersecurity Program [500.02]: Your company has implemented and maintains a cybersecurity program that is:

☐ Designed to protect your company's Information Systems

☐ Based on your company's Risk Assessment[4]

- Designed to perform the following core cybersecurity functions:

  ☐ Identify and assess internal cybersecurity risks

  ☐ Identify and assess external cybersecurity risks

  ☐ Use defensive infrastructure to protect stored Nonpublic Information

  ☐ Detect Cybersecurity Events

  ☐ Respond to detected Cybersecurity Events to mitigate any negative effects

  ☐ Recover from Cybersecurity Events and restore normal operations and services

  ☐ Fulfill applicable regulatory reporting obligations

[4] There is an ambiguity in the DFS regulation: A covered company is required to have a cybersecurity program in place pursuant to 500.02 by August 28, 2017, and certain elements of the program must be based on the covered company's Risk Assessment. However, the Risk Assessments themselves are not actually required until March 1, 2018, i.e., after the program should already be in place. The best practice is likely for covered companies to conduct Risk Assessments by August 28, 2017.

4. Cybersecurity policy [500.03]: Your company has implemented and continues to maintain written policies that:

☐ Are approved by a Senior Officer or board of directors

☐ Are based on your company's Risk Assessment

- Addresses the following areas, as applicable to your company:

  ☐ 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 Third Party Service Provider management

  ☐ Risk assessment

  ☐ Incident response

5. **Incident Response Plan [500.16]: Your company has a written incident response plan that:**

- ☐ Is designed to ensure prompt response to, and recovery from, any Cybersecurity Event that materially affects the confidentiality, integrity or availability of your Information Systems or business operations
- ☐ Addresses the internal process for responding to a Cybersecurity Event
- ☐ Identifies the goals of the plan
- ☐ Addresses external and internal communications and information sharing
- ☐ Identifies requirements for the remediation of any identified weaknesses
- ☐ Provides for documentation and reporting on Cybersecurity Events
- ☐ Allows for the evaluation and revision of the incident response plan after a Cybersecurity Event
- Clearly defines:
  - ☐ Roles
  - ☐ Responsibilities
  - ☐ Levels of decision-making authority

6. **Access Privileges [500.07]:**

- ☐ Your company limits user access to Information Systems as part of the cybersecurity program
- ☐ Your company periodically reviews access privileges

7. **Cybersecurity Personnel and Intelligence [500.10]: Your Company utilizes in-house cybersecurity personnel or third party service provider(s) that:**

- ☐ Manage cybersecurity risks
- ☐ Perform or oversee performance of the company's cybersecurity program
- ☐ Are qualified to manage your company's cybersecurity risks
- ☐ Receive cybersecurity updates and training from your company
- ☐ Maintain current knowledge of cybersecurity issues

Comply by March 1, 2018 / Certify by February 15, 2019

Summary

In addition to the measures listed above, by March 1, 2018, your company must be in compliance with the measures listed below and by February 15, 2019, the board of directors or a senior officer of your company must certify that your company is in compliance with those measures. Specifically, this signed certification would require that your company:

- Require the CISO to prepare a report to your board of directors
- Implement cybersecurity awareness training for personnel
- Implement cybersecurity monitoring and testing
- Conduct a Risk Assessment
- Maintain effective controls to protect Information Systems

Descriptions of Relevant Measures

8. CISO Report [500.04(b)]: Your company's CISO has prepared:

☐ A written report to the board of directors on the cybersecurity program and material risks

- The Report considers, as applicable:
  - ☐ The confidentiality of Nonpublic Information and security of your company's Information Systems
  - ☐ Your company's cybersecurity policies and procedures
  - ☐ Material cybersecurity risks
  - ☐ The overall effectiveness of your company's cybersecurity program
  - ☐ Material Cybersecurity Events involving your company

9. Training [500.14(b)]:

☐ Your company provides regular cybersecurity awareness training for all personnel

☐ The training is updated to reflect risks identified in the risk assessment

10. Penetration Testing and Vulnerability Assessments [500.05]: Your company has incorporated into its cybersecurity program:

- ☐ Monitoring and periodic testing
- ☐ Annual penetration testing
- ☐ Bi-annual vulnerability assessments

11. Risk Assessment [500.09]: Your company has conducted a Risk Assessment for all Information Systems that:

- ☐ Is updated as necessary to address changes in systems, data, and/or business operations
- ☐ Allows for revision of controls in response to evolving threats
- ☐ Is tailored to your company's particular cybersecurity risks and safeguards
- ☐ Is documented
  - Is carried out in accordance with written policies that include
    - ☐ Criteria for evaluating and categorizing identified cybersecurity risks or threats facing the company
    - ☐ Criteria for assessing the confidentiality, integrity, security and availability of your company's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks
    - ☐ Requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks

12. **Multi-Factor Authentication [500.12]: Your company has implemented:**

- ☐ Effective controls, which may include multi-factor authentication or risk-based authentication
- ☐ Multi-factor authentication or a reasonably equivalent or more secure control approved in writing by the CISO for individuals accessing your company's system from an external network

Comply by September 1, 2018 / Certify by February 15, 2019

Summary

In addition to the measures listed above, by September 1, 2018, your company must be in compliance with the measures listed below and by February 15, 2019, the board of directors or a senior officer of your company must certify that your company is in compliance with those measures. Specifically, this signed certification would require that your company:

- Implement audit trails designed to detect and respond to Cybersecurity Events
- Maintain policies and procedures to secure its applications
- Implement controls, including encryption where feasible, to protect nonpublic information
- Monitor authorized users
- Implement limits on data retention

Descriptions of Relevant Measures

13. Audit Trail [500.06]: Your company maintains systems that:

☐ Are able to reconstruct material financial transactions

☐ Maintains records necessary for this purpose for at least five years

☐ Include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of your company

☐ Maintains records necessary for this purpose for at least three years

14. Application Security [500.08]:

☐ Your company's cybersecurity program incorporates:

- Written procedures, guidelines, and standards to ensure the use of secure development practices for in-house applications AND
- Procedures to evaluate the security of externally developed applications used by your company

☐ These procedures are periodically reviewed and updated as necessary by the CISO

15. Encryption of Nonpublic Information [500.15]: To protect Nonpublic Information (at rest or in transit), your company has:

☐ Implemented appropriate controls, including encryption to the extent feasible

- If encryption of information in transit over external networks or at rest is not feasible:
  - ☐ Your company secures Nonpublic Information using effective alternative controls
  - ☐ The alternative controls are reviewed and improved by the CISO
- If your company is using alternative controls:
  - ☐ The CISO reviews the feasibility of encryption and the effectiveness of the alternative controls at least annually.

16. Monitoring [500.14(a)]: Your company has:

☐ Implemented risk-based policies and procedures to monitor the activity of authorized users and detect unauthorized access

17. Limitations on Data Retention [500.13]: For the secure disposal of data, your company has:

☐ Developed policies and procedures for the secure disposal of Nonpublic Information that is no longer necessary for business or legal purposes in the cybersecurity program

Comply by March 1, 2019 / Certify by February 15, 2020

Summary

In addition to the measures listed above, by March 1, 2019, your company must be in compliance with the measures listed below and by February 15, 2020, the board of directors or a senior officer of your company must certify that your company is in compliance with those measures. Specifically, this signed certification would require that your company:

- Maintain a third party service provider policy

Description of Relevant Measure

18. Third Party Service Provider Security Policy [500.11]: Your company implemented a third party service provider policy:

☐ In writing

☐ Based on your company's Risk Assessment

- Addressing the following, to the extent applicable:
  - ☐ Identification and risk assessment of third party service providers
  - ☐ Minimum cybersecurity practices third party service providers must meet to work with your company
  - ☐ Due diligence processes to evaluate third party service providers' cybersecurity
  - ☐ Periodic assessment of the adequacy of third party service providers' cybersecurity
- Including guidelines for due diligence and/or contractual protections relating to third party service providers addressing the following, to the extent applicable:
  - ☐ Third party service providers' policies and procedures for access controls
  - ☐ Third party service providers' policies and procedures for the use of encryption
  - ☐ Notice to your company if there is a cybersecurity event impacting the third party service provider
  - ☐ Representations and warranties about third party service providers' policies and procedures

Appendix A

[Covered Entity Name]

February 15, 20[ ]

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors [or name of Senior Officer(s)] has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the [Board of Directors] or [name of Senior Officer(s)] knowledge, the Cybersecurity Program of [name of Covered Entity as of date of the Board Resolution or Senior Officer(s) Compliance Finding] for the year ended [year for which Board Resolution or Compliance Finding is provided] complies with Part [ ].

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

Name:_____ Date: _____

[DFS Portal Filing Instructions]

Appendix B

Relevant Defined Terms [500.01]

Covered Entity: Anyone operating under or required to operate under an authorization under the Banking Law, the Insurance Law, or the Financial Services Law.

Cybersecurity Event: Any act or attempt to gain unauthorized access to, disrupt, or misuse an Information System or information stored in those systems.

Information System: Discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information, and any specialized system.

Nonpublic Information: All electronic information that is not publically available and is business related, concerns an individual and possible to use to identify that individual, or is data (except age or gender) from a healthcare provider.