Cybersecurity Requirements for Financial Services Companies
Operating Under NY Insurance Law or NY Financial Services Law

1. Determine whether you qualify for a limited exemption. *If applicable, file notice of exemption by August 28, 2017.*

- Exemption applies if: (1) you have fewer than 10 workers located in NY or responsible for our business; (2) you have less than $5 million in gross annual revenue in each of the last three fiscal years from NY business operations of us and our Affiliates; (3) you have less than $10 million in year-end total assets, including assets of all Affiliates; or (4) you do not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information.[1]

2. Maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of our Information Systems. *Compliance required by August 28, 2017.*

- Cybersecurity program must be based on your Risk Assessment and must be designed to perform the following functions: (1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of NPI stored on your Information Systems; (2) use defensive infrastructure and the implementation of policies and procedures to protect your Information Systems and NPI on the Information Systems from unauthorized access or use or other malicious acts; (3) detect Cybersecurity Events; (4) respond to identified or detected Cybersecurity Events to mitigate any negative effects; (5) recover from Cybersecurity Events and restore normal operations and services; and (6) fulfill applicable regulatory reporting obligations.

- Cybersecurity program must include policies and procedures for the secure disposal on a periodic basis of NPI that is no longer necessary for business operations or for other legitimate business purposes, except where such NPI is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the NPI is maintained.

- You should consider whether to have your cybersecurity program cover your employees, agents, representatives, and designees, which will relieve them from having to develop their own cybersecurity programs if they are licensed.

- Cybersecurity program must evaluate and address risks to your Information Systems and NPI that are presented by your Affiliates and subsidiaries.

[1] The requirements discussed in Sections 2-8 generally apply to all insurance licensees regardless of whether qualify for a limited exemption. The fourth exemption is broadest and qualifies an applicable licensees to an exemption from some of the requirements discussed in this memo. The NY cybersecurity requirements place additional requirements on the insurance licensees that do not qualify for one of the exemptions.

3. Implement and maintain a written policy setting forth your policies and procedures for the protection of your Information Systems and NPI stored on the Information Systems. *Compliance required by August 28, 2017.*

- The policy must be based on your Risk Assessment and, to the extent applicable, address the following areas: (1) information security; (2) data governance and classification; (3) asset inventory and device management; (4) access controls and identity management; (5) business continuity and disaster recovery planning and resources; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data privacy; (12) vendor and Third Party Service Provider management; (13) risk assessment; and (14) incident response.

- The policy must be approved by a Senior Officer, the BOD, or an appropriate BOD committee.

- The policy must evaluate and address risks to your Information Systems and NPI that are presented by your Affiliates and subsidiaries.

4. Limit user access privileges to Information Systems that provide access to NPI and periodically review such access privileges. *Compliance required by August 28, 2017.*

5. Annual notice, to be submitted by *February 15, 2018,* certifying that you are in compliance with the requirements of the regulation.

- You must maintain records, schedules, and data supporting the certificate for a period of five years.

- If you identify areas, systems, or processes that require material improvement, updating, or redesign, you must document the identification and the remedial efforts planned and underway to address such areas, systems, or processes.

- Subsequent notices are submitted annually on February 15.

6. Conduct a periodic Risk Assessment of your Information Systems sufficient to inform the design of your cybersecurity program. *Compliance required by March 1, 2018.*

- The Risk Assessment must be documented and carried out in accordance with written policies and procedures. The written policies and procedures must include: (1) criteria for the evaluation and categorization of identified cybersecurity risks or threats; (2) criteria for the assessment of the confidentiality, integrity, security, and availability of your Information Systems and NPI, including the adequacy of existing controls in the context or identified risks; and (3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

- The Risk Assessment must allow for revision of controls to respond to technological developments and evolving threats and must consider the particular risks of your business operations related to cybersecurity, NPI collected or stored, Information Systems, and the availability and effectiveness of controls to protect NPI and Information Systems.
- The Risk Assessment must be updated as reasonably necessary to address changes to your Information Systems, NPI, or business operations.
- The Risk Assessment must evaluate and address risks to your Information Systems and NPI that are presented by your Affiliates and subsidiaries.

7. Provide notice to the NY Superintendent if there is a Cybersecurity Event.

8. Implement written policies and procedures designed to ensure the security of Information Systems and NPI that are accessible to or held by Third Party Service Providers. *Compliance required by March 1, 2019.*

- Policies and procedures must be based on the Risk Assessment and, to the extent applicable, address: (1) the identification and risk assessment of Third Party Service Providers; (2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with us; (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and (4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

- Policies and procedures must include relevant guidelines for due diligence and/or contractual protections relating to Third Party Services including, to the extent applicable, guidelines 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 (may not be required); (3) notice to be provided to us in case of a Cybersecurity Event directly impacting your Information System or NPI 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 your Information Systems or NPI.