Scott A. Sinder
202 429 6289
ssinder@steptoe.com

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.steptoe.com

Steptoe
STEPTOE & JOHNSON LLP

February 21, 2017

TO: The Council of Insurance Agents & Brokers

FROM: Scott A. Sinder
Eva V. Rigamonti
Joshua M. Oppenheimer

RE: **New York State Department of Financial Services – Final Cybersecurity Regulation**

On February 16, 2017, the New York State Department of Financial Services (NYSDFS) published the final version of its cybersecurity rule (the "Rule") requiring any individual, partnership, corporation, association, or any other entity "*operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law,* ***the Insurance Law*** *or the Financial Services Law*" to establish and maintain cybersecurity programs as required by the regulation to protect their systems and data.[1] Both carriers and agency/brokerage firms are subject to this Rule. Failure to comply could subject covered entities to NYSDFS enforcement proceedings.

The proposed rule was widely criticized as being overly prescriptive and deviating from federal and other widely accepted requirements and protocols. The final Rule generally is substantively identical to the last version of the proposed rule but with one very notable exception: the exemptions have been modified to provide that firms (and their affiliates) with —

1. fewer than 10 employees (including independent contractors) **located in New York**; or
2. less than $5,000,000 in gross annual revenue in each of the prior three fiscal years **from New York business operations**; or
3. less than $10,000,000 in year-end total assets

are completely exempt from many of the more onerous and prescriptive components of the Rule (the "Small New York Business" Exemption).[2]

As discussed in more detail below, the Rule generally requires:

[1] New York Department of Financial Services, Final Rule, Cybersecurity Requirements for Financial Services Companies, §§ 500.01(c),(i); 500.02; *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf.

[2] § 500.19(a) ("Small New York Business" Exemption).

1. A **cybersecurity program** based on the risk assessment of the covered entity;
2. A written **cybersecurity policy** approved by each entity’s senior officer or board of directors;
3. Periodic **risk assessments** to inform design of the cybersecurity program;
4. Policies and procedures applicable to **third-party vendors**;
5. Proper **notices to the NYSDFS Superintendent** within 72 hours of a “cybersecurity event;”[3]
6. A **Chief Information Security Officer** appointed by each entity to implement the cybersecurity program and oversee qualified cybersecurity personnel;
7. Testing of the program’s **penetration and vulnerability**;
8. An **audit trail** for all cybersecurity activity;
9. Procedures for ensuring in-house developed **application** security;
10. **Monitoring** of user access;
11. Multi-factor **authentication procedures** for user access and **encryption** of nonpublic information;
12. A written **incident response plan** to respond to any material cybersecurity event; and
13. Regular cybersecurity awareness **training**.

Covered entities that qualify under the Small New York Business Exemption parameters noted above and that submit a Notice to the NYSDFS notifying the Department that they qualify for the exemption are subject to a significantly reduced set of obligations under the Rule and need only comply with the first five sets of requirements listed above. Such firms thus are not, for example, required to: have a Chief Information Security Officer; test their cybersecurity program’s penetration and vulnerability; maintain an audit trail of all cybersecurity activity; utilize multi-factor authentication procedures for user access or encrypt nonpublic information.

Technically, the Rule goes into effect on March 1, 2017, but covered entities generally will have until <u>August 28, 2017</u> to transition into compliance with it.[4] The Rule further provides delayed compliance dates for many of the specific requirements as follows:

- <u>February 15, 2018</u> for the annual Certification of Compliance notice to the NYSDFS Superintendent (§ 500.17(b));
- <u>March 1, 2018</u> for the Chief Information Security Officer reporting requirements (§ 500.04(b)), penetration testing and vulnerability assessments (§ 500.05), risk

[3] A “cybersecurity event” is any act or attempt to gain unauthorized access to disrupt an information system or information on that system. § 500.01(d) (Cybersecurity Event).

[4] § 500.21 (Effective Date); § 500.22 (Transitional Periods).

assessment obligations (§ 500.09), multi-factor authentication requirements (§ 500.12), and select cybersecurity training requirements (§ 500.14(b));

- September 1, 2018 for audit trail requirements (§ 500.06), application security requirements (§ 500.08), limitations on data retention (§ 500.13), certain monitoring requirements (§ 500.14(a)), and encryption requirements (§ 500.15); and
- March 1, 2019 for Third Party Service Provider policy requirements (§ 500.11).

The Rule analysis below is divided into three parts:

1. Part A outlines the requirements applicable to all covered entities, including those that qualify for the Small New York Business Exemption, unless another exemption applies;

2. Part B discusses the additional requirements applicable to "non-exempt" covered entities (i.e. covered entities that do not qualify for the Small New York Business Exemption); and

3. Part C sets forth the procedure for qualifying for an exemption and includes a chart listing all of the exemptions to the Rule and the scope of each exemption.

Analysis

A. Requirements Applicable To All Covered Entities[5]

1. **Cybersecurity Program** (§§ 500.02; 500.07; 500.13)

All covered entities (including those that qualify for the Small New York Business Exemption) must establish and maintain a **cybersecurity program** based on their **risk assessments** (described below in Section A.3) to ensure the confidentiality and integrity of their "information systems."[6] They may either create their own cybersecurity programs or adopt the relevant and applicable provisions of one maintained by an affiliate.[7] An "affiliate" is any individual or non-governmental entity "that

[5] As outlined in Section C below, there are exemptions beyond the Small New York Business Exemption that may apply to limit or eliminate the application of the Rule to other covered entities.

[6] § 500.02(a) (Cybersecurity Program). "Information System" is broadly defined as any "set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." § 500.01(e) (Information System).

[7] § 500.02(c) (Cybersecurity Program).

controls, is controlled by, or is under common control with another" individual or non-governmental entity.[8]

An entity's cybersecurity program must be designed to perform the following core cybersecurity functions (with appropriate verifying documentation to be made available to the NYSDFS Superintendent upon request):[9]

- Identify and assess cybersecurity risks that could threaten the security or integrity of "nonpublic information"[10] stored on the entity's systems;
- Implement defensive infrastructure and policies to protect against unauthorized access and use (including periodically reviewing who has access to nonpublic information);[11]
- Detect cybersecurity events;
- Respond to and mitigate any incidents;
- Recover from cybersecurity incidents and restore normal operations; and
- Fulfill all regulatory obligations.[12]

All covered entities also must further implement policies and procedures for the **secure disposal** on a periodic basis of any nonpublic information that is no longer necessary for business operations, except where such information must be retained by law or regulation, or where such disposal is not reasonably feasible due to the manner in which it is maintained.[13]

[8] § 5001.01(a) (Affiliate). Control means "the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a[n individual or non-governmental entity], whether through the ownership of stock of such [individual or non-governmental entity] or otherwise." *Id.*

[9] § 500.02(d) (Cybersecurity Program). The Rule does not elaborate on what type of documentation must be made available.

[10] "Nonpublic information" is broadly defined in the Rule, encompassing (1) any business related information the tampering with which would cause a material adverse impact to the business; (2) any information that could identify an individual when combined with the individual's social security number, drivers' license number, account number, security or access code, or biometric records; and (3) any information, except for age or gender, derived from a health care provider or an individual that relates to the physical, mental, or behavioral health of the individual or his family, his health care, or payment of his health care. § 500.01(g) (Nonpublic Information).

[11] § 500.07 (Access Privileges). "Periodically" is not further defined other than by the regulatory text.

[12] § 500.02(b) (Cybersecurity Program).

[13] § 500.13 (Limitations on Data Retention).

2. **Cybersecurity Policy** (§ 500.03)

All covered entities must create and implement a **written cybersecurity policy**, approved by each firm's "senior officer"[14] or board of directors, that sets forth their policies and procedures to protect their information systems and nonpublic information stored on those systems.[15]

The policy must be based on the covered entity's **risk assessment** and address the following areas, to the extent applicable: (a) information security, (b) data governance and classification, (c) asset inventory and device management, (d) access controls and identity management, (e) business continuity and disaster recovery planning resources, (f) systems operations and availability concerns, (g) systems and network security, (h) systems and network monitoring, (i) systems and application development and quality assurance, (j) physical security and environmental controls, (k) customer data privacy, (l) vendor and Third Party Service Provider (described below in Section A.4) management, (m) risk assessment, and (n) incident response.

3. **Risk Assessments** (§ 500.09)

All covered entities must conduct periodic, documented **risk assessments** of their systems, sufficient to inform the design of their cybersecurity programs.[16] These risk assessments must be updated as reasonably necessary to address changes to an entity's information systems, nonpublic information, and business operations. The risk assessments also must allow for revision of controls to respond to technological developments and evolving threats, and must consider the particular risks of a covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized, and the availability and effectiveness of controls to protect nonpublic information and information systems.

Each risk assessment must be carried out in accordance with written policies and procedures, including: (1) criteria for the evaluation and categorization of identified risks or threats; (2) criteria for the assessment of the confidentiality, integrity, security, and availability of the entity's systems (including the adequacy of existing controls in the context of 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 those risks).

[14] A "senior officer" is defined as "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 Rule. § 500.01(m) (Senior Officer(s)).

[15] § 500.03 (Cybersecurity Policy). Under the original proposal, an entity's cybersecurity policy would have needed to be reviewed and approved by *both* the entity's senior officer and board of directors.

[16] §500.09 (Risk Assessment). Under the initial proposal, covered entities would have been required to conduct at least one risk assessment per year and would have been forced to document and justify decisions regarding how they would mitigate identified risks.

4. **Third Party Service Providers** (§ 500.11)

All covered entities must implement written policies and procedures designed to ensure the security of information systems and nonpublic information accessible to or held by **Third Party Service Providers (TPSPs)**.[17] A TPSP is any individual or non-governmental entity 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.[18]

Such policies and procedures must be based on the covered entity's risk assessment and address, to the extent applicable, the identification and risk assessment of these TPSPs, and the minimum cybersecurity practices required to be met by them before they can do business with the covered entity. A covered entity must further conduct due diligence and periodic assessments of the adequacy of TPSPs' cybersecurity practices.

In addition, such policies and procedures also must include relevant guidelines for due diligence and/or contractual provisions relating to TPSPs, addressing the TPSPs' policies and procedures for access controls, including their use of multi-factor authentication and encryption if the covered entity is non-exempt and thus also subject to these requirements (see Part B below). The guidelines also must address when the TPSP must provide notice to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or the covered entity's nonpublic information that is held by the TPSP, and representations and warranties addressing the TPSPs' cybersecurity policies and procedures as they relate to the security of the covered entity's systems and information.[19]

5. **Notices to the NYSDFS Superintendent** (§§ 500.17; 500.18; 500.19(e),(g))

Finally, all covered entities must provide a **notice to the NYSDFS Superintendent** within 72 hours of a cybersecurity event that has a reasonable likelihood of materially affecting the entity's normal operations or where notice to another governmental body, self-regulatory agency, or supervisory body is required.[20] Covered entities also must file a **written Certification of Compliance** with the Superintendent by February 15 each year stating that it is in compliance with the Rule, and maintain

[17] § 500.11 (Third Party Service Provider Security Policy).

[18] § 500.01(n) (Third Party Service Provider(s)).

[19] While covered entities have flexibility to deal with TPSPs, it is unclear how an entity with limited leverage would be able to periodically assess a large vendor's policies.

[20] §500.17 (Notices to Superintendent). Under the revised proposal, the NYSDFS limited the types of events that must be reported to only include those cybersecurity events where there was a likelihood of a material effect on the entity's operations and where notice to another governmental body, self-regulatory agency, or supervisory body was required. In its final Rule, the Department reverted back to its original proposal requiring notice within 72 hours when *either* prong is met, which will likely result in more reports than would have been filed under the revised proposal.

documentation supporting this Certification for five years.[21] If a covered entity identifies areas, systems, or processes that require material improvement, updating, or redesign, it must document this and make such documentation available for the Superintendent's inspection.

The Rule clarifies – albeit cursorily – that confidential information shared with the NYSDFS is subject to exemptions from disclosure under the "Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law," such as the Freedom of Information Act.[22]

B. Requirements Applicable To Covered Entities That Do Not Qualify For The Small New York Business Exemption (Or Another Exemption)

1. Chief Information Security Officer and Cybersecurity Personnel (§§ 500.04; 500.10)

Non-exempt covered entities must appoint a **Chief Information Security Officer (CISO)** to be responsible for implementing, overseeing, and enforcing their cybersecurity programs and policies.[23] The CISO's responsibilities may be handled by a Third Party Service Provider, so long as the entity retains accountability over the CISO's duties and designates a senior member of the entity to ensure that the third party complies with the CISO requirements.

The CISO's duties include developing and filing a report at least annually[24] to the entity's board of directors or, if the entity does not have a board of directors, to the entity's senior officer. The report must cover the entity's cybersecurity program and material cybersecurity risks, including (1) the integrity and security of the entity's systems, (2) its policies and procedures, (3) material cybersecurity risks to the entity, (4) overall effectiveness of the entity's cybersecurity program, and (5) material cybersecurity events in the reported period.

In addition to the appointment of a CISO, non-exempt covered entities must use **qualified cybersecurity personnel** sufficient to manage the entities' cybersecurity risks and assist the CISOs in implementing the entities' cybersecurity programs.[25] Non-exempt covered entities must further provide these personnel with sufficient training to address relevant risks, and verify that key personnel are taking

[21] The Certification of Compliance covered entities must submit is set forth as Appendix A in the final Rule. As The Council noted in its comments to the NYSDFS, the annual certification requirement does not provide an option to certify that an entity is working to remediate a point of weakness uncovered during a risk assessment, or define the personal liability if the entity is ultimately found to be noncompliant.

[22] § 500.18 (Confidentiality). This provision was added in the revised proposal as a result of comments received from The Council and others. There is no HIPAA exemption.

[23] § 500.04 (Chief Information Security Officer).

[24] The final Rule scaled back the original proposed requirement that would have required the CISO to submit his report at least twice a year.

[25] § 500.10 (Cybersecurity Personnel and Intelligence). "Qualified cybersecurity personnel" is not explained other than by the regulatory text.

steps to maintain their current knowledge of changing cybersecurity threats and countermeasures. Like the appointment of their CISOs, non-exempt covered entities may use affiliates or Third Party Service Providers to comply with these cybersecurity personnel requirements.

2. **Testing of the Program's Penetration and Vulnerability** (§ 500.05)

Non-exempt covered entities must perform continuous system monitoring or periodic **penetration and vulnerability assessments** to evaluate the effectiveness of their cybersecurity programs.[26] *If, however, an entity cannot perform effective continuous monitoring, it must conduct annual penetration testing and bi-annual vulnerability assessments*.

3. **Audit Trail** (§ 500.06)

Non-exempt covered entities must maintain, to the extent applicable and based on their risk assessments, **audit trails** for all cyber activity. The Rule points to two different types of audit trails: audit trails designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the covered entity, and 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 the entity. Audit trails designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the entity must be kept for at least five years, while 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 the entity must be kept for at least three years.[27]

4. **Application Security** (§ 500.08)

Non-exempt covered entities must have written procedures, guidelines, and standards designed to ensure the use of secure development practices for their own applications, and procedures for evaluating, assessing, or testing the security of externally developed applications.[28] All such procedures, guidelines, and standards must be reviewed, assessed, and updated as necessary by the Chief Information Security Officer (described above in Section B.1).

[26] § 500.05 (Penetration Testing and Vulnerability Assessments). "Penetration Testing" means "a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration databases or controls from outside or inside the Covered Entity's Information Systems." § 500.01(h) (Penetration Testing). The original proposal would have required, at a minimum, at least annual penetration testing and at least quarterly vulnerability assessments.

[27] § 5001.06 (Audit Trail). The final Rule significantly scales back the audit requirements that had been initially proposed. Instead of requiring constant data tracking and logging, the Rule now requires entities to conduct audits "to the extent applicable and based on its Risk Assessment." *Id.* The final Rule also reduced data retention for audit trails designed to detect cybersecurity events from five to three years.

[28] § 500.08 (Application Security).

5. **Training/Monitoring** (§ 500.14)

Non-exempt covered entities must implement risk-based policies, procedures, and controls designed to **monitor** "authorized users,"[29] detect unauthorized access, and the use of or tampering with nonpublic information. Covered entities also must provide regular, updated cybersecurity awareness **training** to reflect the risks identified in the entities' risk assessments.[30]

6. **Multi-Factor Authentication and Encryption** (§§ 500.12; 500.15)

Non-exempt covered entities must, based on their risk assessments, use effective controls to protect against unauthorized access to nonpublic information or information systems. **Multi-factor authentication** must be utilized for any individual accessing a covered entity's internal networks from an external network, unless the CISO approves (in writing) at least reasonably equivalent access controls.[31] Multi-factor authentication means authentication through verification of at least two of the following: (1) Knowledge, such as a password; (2) Possession factors, such as a token or text message on a mobile phone; or (3) Inherence factors, such as a biometric characteristic.[32]

Non-exempt covered entities also must **encrypt** all nonpublic information, both in transit and at rest. If this is infeasible, the entity may instead secure its nonpublic information using effective alternative compensating controls approved by the CISO and annually reviewed.[33]

7. **Incident Response Plan** (§ 500.16)

Finally, non-exempt covered entities must create a **written incident response plan** to respond to any material cybersecurity event affecting the confidentiality, integrity, or availability of their systems or continuity of their businesses.[34] This incident response plan must address the internal processes for responding to a cybersecurity event and the goals of the response plan. The plan must further:

- Clearly define the roles, responsibilities, and levels of decision-making authority;
- Coordinate internal and external communications;

[29] An "authorized user" is any employee, contractor, agent, or other individual or non-governmental entity that participates in the business of a covered entity and is authorized to access and use any information systems and data of the covered entity. § 500.01(b) (Authorized User).

[30] § 500.14 (Training and Monitoring). The Rule does not elaborate any further on the extent of this training.

[31] §5001.12 (Multi-Factor Authentication). The final Rule's shift, from always requiring multi-factor authentication to a risk-based approach permitting entities to use "effective controls" that may include multi-factor authentication, will provide greater flexibility to businesses to choose the most effective tool (in terms of both cost and security) to protect their networks and data.

[32] § 500.01(f) (Multi-Factor Authentication).

[33] § 500.15 (Encryption of Nonpublic Information).

[34] § 500.16 (Incident Response Plan).

- Identify requirements for remediation of weaknesses in the system;
- Document and report cybersecurity events and the entity's response to those events to the appropriate regulatory authorities;[35] and
- Evaluate and improve incident response plans following a cybersecurity event.

C. **Exemptions** (§ 500.19)

The Rule provides for a number of **exemptions** for certain covered entities. Covered entities wishing to qualify for an exemption generally must file a Notice of Exemption (in the form set forth in Appendix B of the Rule) within 30 days after they determine they are exempt.[36] If a covered entity subsequently ceases to qualify for an exemption, it will have 180 days to come into compliance with the Rule.[37] The covered entities that may qualify for exemption and the scope of those exemptions are as follows:[38]

Covered Entity	**Exempted Provision(s) of the Rule**
• Entities subject to Insurance Law § 1110 (Charitable Annuity Societies); or • Entities subject to Insurance Law § 5904 (Risk Retention Groups Not Charted in New York); or • Any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125 (Credit for Reinsurance from Unauthorized Insurers) — provided the entity does not otherwise qualify under the Rule.[39]	Exempt from all provisions.
An employee, agent, representative, or designee of a covered entity, who is himself a covered entity.[40]	Exempt from all provisions to the extent he is covered by the covered entity's cybersecurity program.

[35] The Rule does not further elaborate regarding to whom such reporting must be made.

[36] The 30 day limit was added in the final Rule.

[37] §§ 500.19(e), (g) (Exemptions).

[38] § 500.19 (Exemptions).

[39] § 500.19(f). This exemption was added in the final Rule and it appears that covered entities qualifying for this exemption need not file the Appendix B Notice.

[40] § 500.19(b).

• A covered entity that does not operate, maintain, utilize, or control any information systems and that does not and is not required to control, own, access, generate receive, or possess nonpublic information;[41] or • A covered entity under Insurance Law Article 70 (Captive Insurance Companies) that does not and is not required to control, own, access, generate, receive, or possess nonpublic information other than information relating to its corporate parent company (or affiliates).[42]	Exempt from all provisions *except* • Risk Assessment (§ 500.09); • TPSPs (§ 500.11); • Limitations on Data Retention (§ 500.13); and • Notices to Superintendent (§ 500.17).
"Small New York Business" Exemption. Firms (and their affiliates) with — • Fewer than 10 employees (including independent contractors) located in New York or responsible for business of the covered entity; or • Less than $5 million in gross annual revenue in each of the prior three fiscal years from New York business operations; or • Less than $10 million in year-end total assets.[43]	Exempt from the following provisions: • CISO (§ 500.04); • Penetration Testing and Vulnerability Assessments (§ 500.05); • Audit Trail (§ 500.06); • Application Security (§ 500.08); • Cybersecurity Personnel and Intelligence (§ 500.10); • Multi-Factor Authentication (§ 500.12); • Training and Monitoring (§ 500.14); • Encryption of Nonpublic Information (§ 500.15); and • Incident Response Plan (§ 500.16).

[41] § 500.19(c).

[42] § 500.19(d).

[43] § 500.19(a).