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
Updated January 8, 2019

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**

***NB**: This memorandum was updated on January 8, 2019, to incorporate relevant information contained in Frequently Asked Questions published on the NYSDFS website,[1] as well as to clarify the Rule's exemptions (see Part C below).*

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.[2] 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

---

[1] New York State Department of Financial Services, Frequently Asked Questions Regarding 23 NYCRR Part 500, *available at* https://www.dfs.ny.gov/about/cybersecurity_faqs.htm [hereinafter "NYSDFS FAQ"].

[2] 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.

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).[3]

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

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;"[4]
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 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 August 28, 2017 to transition into compliance with it.[5] The Rule further provides delayed compliance dates for many of the specific requirements as follows:

[3] § 500.19(a) ("Small New York Business" Exemption).

[4] 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).

- February 15, 2018 for the annual Certification of Compliance notice to the NYSDFS Superintendent (§ 500.17(b));
- March 1, 2018 for the Chief Information Security Officer reporting requirements (§ 500.04(b)), penetration testing and vulnerability assessments (§ 500.05), risk 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[6]

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."[7] They may either create their own cybersecurity programs or adopt the relevant and applicable provisions of

[5] § 500.21 (Effective Date); § 500.22 (Transitional Periods).

[6] 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.

[7] § 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).

one maintained by an affiliate.[8] An "affiliate" is any individual or non-governmental entity "that controls, is controlled by, or is under common control with another" individual or non-governmental entity.[9] When a subsidiary or other affiliate of a covered entity presents risks to the covered entity's information systems or the nonpublic information stored on those information systems, those risks must be evaluated and addressed in the covered entity's risk assessment, cybersecurity program, and cybersecurity policies.[10]

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):[11]

- Identify and assess cybersecurity risks that could threaten the security or integrity of "nonpublic information"[12] 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);[13]
- Detect cybersecurity events;
- Respond to and mitigate any incidents;
- Recover from cybersecurity incidents and restore normal operations; and
- Fulfill all regulatory obligations.[14]

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,

[8] § 500.02(c) (Cybersecurity Program). A covered entity may adopt an affiliate's cybersecurity program in whole or in part, as long as the covered entity's overall cybersecurity program meets all requirements of the Rule. NYSDFS FAQ at Question 26.

[9] § 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.*

[10] NYSDFS FAQ at Question 22.

[11] § 500.02(d) (Cybersecurity Program). The Rule does not elaborate on what type of documentation must be made available.

[12] "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).

[13] § 500.07 (Access Privileges). "Periodically" is not further defined other than by the regulatory text.

[14] § 500.02(b) (Cybersecurity Program).

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.[15]

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

All covered entities must create and implement a **written cybersecurity policy**, approved by each firm's "senior officer"[16] or board of directors, that sets forth their policies and procedures to protect their information systems and nonpublic information stored on those systems.[17]

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.[18] 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

[15] § 500.13 (Limitations on Data Retention).

[16] 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)).

[17] § 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.

[18] §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.

describing how identified risks will be mitigated or accepted based on the risk assessment (and how the cybersecurity program will address those 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)**.[19] 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.[20] It is possible that the same entity can be a covered entity, an authorized user, and a TPSP – all at the same time.[21]

The TPSP 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. Solely relying on a TPSP's Certification of Compliance (see Section 5 below) will not be adequate due diligence.[22]

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).[23] 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. Likewise, the guidelines must specify the representations and warranties necessary for the TPSPs' cybersecurity policies and procedures as they relate to the security of the Covered Entity's systems and information.[24]

[19] § 500.11 (Third Party Service Provider Security Policy).

[20] § 500.01(n) (Third Party Service Provider(s)).

[21] NYSDFS FAQ at Questions 2, 36. This may force some covered entities to duplicate or expand their cybersecurity program beyond what is required of them under the Rule. For additional discussion on this topic, see our January 8, 2019 addendum memorandum.

[22] NYSDFS FAQ at Question 13.

[23] NYSDFS FAQ at Question 37.

[24] 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.

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.[25] According to the NYSDFS FAQs, at a minimum, an unsuccessful attack should be reported when it is sufficiently serious to raise a concern[26]—and a covered entity is required to give notice when a cybersecurity event involves harm to consumers.[27]

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 documentation supporting this Certification for five years.[28] The Certification requirement may not be met by an affiliate certifying compliance on behalf of the covered entity.[29] 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. Individuals that qualify as covered entities and are filing a Certification for their own individual license are acting as Senior Officers[30] and should complete the Certification process in that manner.[31] There is no need to submit explanatory or additional materials with the Certification, but the covered entity should maintain the documents and records necessary that support the certification because NYSDFS could request the information in the future.[32]

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,

---

[25] §500.17 (Notices to Superintendent); NYSDFS FAQ at Question 34. 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.

[26] NYSDFS FAQ at Question 20.

[27] *Id.* at Question 24. Its cybersecurity program and policies also should address notice to consumers in order to be consistent with the risk-based requirements of the Rule. *Id.* at Question 25.

[28] 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. A covered entity may not submit a Certification unless it is in compliance with all applicable requirements of the Rule *at the time of certification*. *Id.* at Question 32.

[29] *Id.* at Question 27.

[30] A Senior Officer is "the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems and/or risk of a Covered Entity . . . ." § 500.01(m).

[31] NYSDFS FAQ at Question 6.

[32] *Id.* at Question 15.

Public Officers Law or any other applicable state or federal law," such as the Freedom of Information Act.[33]

Notices of cybersecurity events, Certifications of Compliance, and Notices of Exemptions (see Part C below) should be filed electronically via the DFS Web Portal.[34] In the Portal, the Entity ID is a user's unique license or charter number issued by the State of New York.[35] Insurance companies' Entity ID will be their NAIC numbers. Insurance producers are not to include the leading alpha characters of their license number (e.g., BR, IA, LA, PC, TLA).

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.[36] 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.[37]

The CISO's duties include developing and filing a report at least annually[38] to the entity's board of directors[39] 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

---

[33] § 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.

[34] NYSDFS FAQ at Question 35.

[35] *Id.* at Question 7.

[36] § 500.04 (Chief Information Security Officer).

[37] To the extent a covered entity utilizes an employee of an affiliate to serve as the covered entity's CISO, the affiliate is not considered a TPSP. NYSDFS FAQ at Question 28.

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

[39] This requirement cannot be met by reporting to an authorized subcommittee of the board. *Id.* at Question 18.

implementing the entities' cybersecurity programs.[40] Non-exempt covered entities must further provide these personnel with sufficient training to address relevant risks, and verify that key personnel are taking 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.[41] *If, however, an entity cannot perform effective continuous monitoring,[42] 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.[43]

---

[40] § 500.10 (Cybersecurity Personnel and Intelligence). "Qualified cybersecurity personnel" is not explained other than by the regulatory text.

[41] § 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.

[42] According to the NYSDFS FAQs, effective continuous monitoring could be attained through a variety of technical and procedural tools, controls, and systems. NYSDFS FAQ at Question 33. There is no specific technology that is required to be used in order to have an effective program. Effective continuous monitoring generally has the ability to continuously, on an ongoing basis, detect changes or activities within a covered entity's information systems that create or indicate the existence of cybersecurity vulnerabilities or malicious activity. In contrast, non-continuous monitoring of information systems, such as through periodic manual review of logs and firewall configurations, would not be considered effective continuous monitoring.

[43] § 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.

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.[44] 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).

5. **Training/Monitoring** (§ 500.14)

Non-exempt covered entities must implement risk-based policies, procedures, and controls designed to **monitor** "authorized users,"[45] 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.[46]

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.[47] 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.[48]

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.[49]

---

[44] § 500.08 (Application Security).

[45] 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).

[46] § 500.14 (Training and Monitoring). The Rule does not elaborate any further on the extent of this training.

[47] §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.

[48] § 500.01(f) (Multi-Factor Authentication).

[49] § 500.15 (Encryption of Nonpublic Information). On December 21, 2018, NYSDFS issued a memo highlighting the importance of access controls like those required in §§ 500.12, 500.14, and 500.15 of the Rule. *See* New York State Department of Financial Services, Memorandum, DFS Cybersecurity Regulation – First Two Years and Next Steps (Dec. 21, 2018) at 3, *available at* https://www.dfs.ny.gov/about/cyber_memo_12212018.pdf.

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.[50] 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;
- 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;[51] and
- Evaluate and improve incident response plans following a cybersecurity event.

C. Exemptions (§ 500.19)

The Rule provides four different **exemptions** for certain covered entities. Some exemptions require the exempt entity to file a Notice of Exemption, and some require the exempt entity to still file a separate Certification of Compliance. The four exemptions are summarized below, and the first two exemptions are detailed further in the accompanying chart.

The **first exemption** – most likely applicable to many Council members – we have dubbed the "Small New York Business" exemption.[52] Under this exemption, covered entities with (1) fewer than 10 employees (including independent contractors) located in New York; (2) less than $5,000,000 in gross annual revenue in each of the prior three fiscal years; or (3) less than $10,000,000 in year-end total assets, are exempt from many of the more onerous and prescriptive components of the Rule. *However*, these covered entities must still comply with some of the Rule's requirements, including the requirement to establish and maintain a cybersecurity program.[53]

The **second exemption** applies to covered entities that do not operate, maintain, utilize, or control any information systems and that do not and are not required to control, own, access, generate, receive, or possess nonpublic information;[54] and covered entities under Insurance Law Article 70 (Captive Insurance Companies) that do not and are not required to control, own, access, generate,

[50] § 500.16 (Incident Response Plan).

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

[52] § 500.19(a); NYSDFS FAQ at Question 3.

[53] *See also* NYSDFS FAQ at Question 23 (explaining that covered entities that qualify for an exemption are only exempt from complying with certain provisions as set forth in the Rule, and must comply with the sections listed in the exemption that apply to that covered entity).

[54] § 500.19(c); NYSDFS FAQ at Question 3.

receive, or possess nonpublic information other than information relating to their corporate parent companies (or affiliates).[55] These covered entities are similarly exempt from some, but not all, of the Rule's requirements.[56]

The Rule's first two exemptions and their remaining compliance requirements are detailed further in the below chart. Of note, a covered entity that qualifies for either the first or second exemption, and submits its Notice of Exemption, must still file an annual Certification of Compliance by February 15 of each year.[57]

The **third exemption** applies to employees, agents, representatives, and designees of covered entities, who themselves are covered entities.[58] These individuals are exempt from all requirements of the Rule to the extent they are covered by their respective covered entity's cybersecurity program.[59] A covered entity qualifying for the third exemption still must file a Notice of Exemption but does not have to file a Certification of Compliance.

Finally, the **fourth exemption** applies to: (1) entities subject to Insurance Law § 1110 (Charitable Annuity Societies); (2) entities subject to Insurance Law § 5904 (Risk Retention Groups Not Chartered in New York); and (3) 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 entities do not otherwise qualify under the Rule.[60] These entities also are exempt from all requirements of the Rule, and do not have to file a Notice of Exemption or a Certification of Compliance.

Except for those entities qualifying for the fourth exemption, any covered entity that wishes to qualify for an exemption must file a Notice of Exemption within 30 days after they determine they are exempt.[61] Recently, NYSDFS made clear that the Notice of Exemption requirement is an *annual* obligation. All covered entities that previously filed for an exemption, therefore, must **re-file**

---

[55] § 500.19(d); NYSDFS FAQ at Question 3.

[56] *See also* NYSDFS FAQ at Question 23.

[57] § 500.17(b); *see also* New York State Department of Financial Services, Key Questions About the Recent Cyber Regulation Notice, *available at* https://www.dfs.ny.gov/about/cybersecurity.htm.

[58] § 500.19(b).

[59] If the covered entity is an employee, agent, representative, or designee of more than one covered entity, it will only qualify for this exemption where the cybersecurity program of at least one of its parent covered entities *fully* covers all aspects of the employee's, agent's, representative's, or designee's business. NYSDFS FAQ at Question 16.

By permission, NYSDFS will approve certain covered entities to file notices of exemption on behalf of their employees or captive agents who also are covered entities. NYSDFS FAQ at Question 19. This option is only available for filings of 50 or more employees or captive agents and only if all employees or captive agents qualify for the same exemptions. *Id.* See NYSDFS FAQ at Question 19 for additional requirements.

[60] § 500.19(f).

[61] § 500.19(e); NYSDFS FAQ at Question 17.

their Notice of Exemption if they wish to keep their exempt status, and must do so ***prior* to submitting their annual Certification of Compliance due by February 15, 2019**. (To be clear, the Notice of Exemption and the Certification of Compliance – both due annually – are two separate submissions, and the Notice of Exemption must be filed *before* the Certification of Compliance.[62]) If a covered entity needs to amend its Notice of Exemption in the event of changes after the initial submission (e.g., name changes or changes to the applicable exemption(s)), it should submit a new Notice of Exemption, which would not be considered an amendment to the original submission.[63] If a covered entity subsequently ceases to qualify for an exemption, it will have 180 days to come into compliance with the Rule.[64]

Exemptions #1 and #2 and Their Resulting Compliance Requirements

(Because Exemptions #3 and #4 exempt entities from all of the Rule's requirements, they are not included in this chart.)

Covered Entities Must Comply With (✔) . . .	**No Exemption**	**Exemption #1 *"Small New York Business" Exemption***	**Exemption #2**
Cybersecurity Program (§ 500.02)	✔	✔	
Cybersecurity Policy (§ 500.03)	✔	✔	
CISO (§ 500.04)	✔		
Penetration Testing and Vulnerability Assessments (§ 500.05)	✔		
Audit Trail (§ 500.06)	✔		
Access Privileges (§ 500.07)	✔	✔	
Application Security (§ 500.08)	✔		
Risk Assessment (§ 500.09)	✔	✔	✔

[62] It is advised that covered entities file their Notice of Exemption in January to allow time for NYSDFS to process the Notice prior to the subsequent Certification of Compliance filing due by February 15, 2019.

Both the Notice of Exemption and the Certification of Compliance must be filed electronically via the NYSDFS cybersecurity portal. Make sure you have your identifying number (i.e., NYS License number, NAIC/NY Entity number, NMLS number or Institution number) available when you make your filing. A look-up feature is included in the portal for anyone who does not know which number to use. Access to the portal and additional information on how to file can be found here: https://www.dfs.ny.gov/about/cybersecurity.htm.

After filing, you will receive an email that includes a receipt number for all filings you complete. The receipt will indicate the year the filing was made. The receipt will also indicate the type of filing made: Notices of Exemption will have a receipt number that begins with the letter "E." Certifications of Compliance will have a receipt number that starts with the letter "C." It is suggested that you maintain a copy of this email in your records for future reference.

[63] NYSDFS FAQ at Question 14. For example, if a covered entity originally submitted a Notice of Exemption stating that it qualified for the third exemption and the "New York Small Business" exemption, but it now only qualifies for the "New York Small Business" exemption, then the covered entity must submit a new Notice of Exemption with the correct information. The Notices of Exemptions should be filed electronically, and the covered entity should use the account it used to file the original Notice of Exemption.

[64] §500.19(g).

Covered Entities Must Comply With (✔) . . .	**No Exemption**	**Exemption #1** ***"Small New York Business" Exemption***	**Exemption #2**
Cybersecurity Personnel and Intelligence (§ 500.10)	✔		
Third Party Service Provider Security Policy (§ 500.11)	✔	✔	✔
Multi-Factor Authentication (§ 500.12)	✔		
Limitations on Data Retention (§ 500.13)	✔	✔	✔
Training and Monitoring (§ 500.14)	✔		
Encryption of Nonpublic Information (§ 500.15)	✔		
Incident Response Plan (§ 500.16)	✔		
Notices to Superintendent (§ 500.17), *includes Certification of Compliance*	✔	✔	✔
Confidentiality (§ 500.18)	✔	✔	✔
Exemptions (§ 500.19)	✔	✔	✔
Enforcement (§ 500.20)	✔	✔	✔
Effective Date (§ 500.21)	✔	✔	✔
Transitional Periods (§ 500.22)	✔	✔	✔
Severability (§ 500.23)	✔	✔	✔