

## Regulatory Impact Statement for Proposed New 23 NYCRR 500.

1. Statutory Authority: In Section 102 of the New York Financial Services Law (the “Financial Services Law” or “FSL”), the legislature declares that the purpose of the FSL is “to ensure the continued safety and soundness of New York’s banking, insurance and financial services industries, as well as the prudent conduct of the providers of financial products and services, through responsible regulation and supervision.” Pursuant to FSL Section 201, the Department of Financial Services (the “Department”) has broad authority to take such actions as are necessary to ensure the continued solvency, safety, soundness and prudent conduct of the providers of financial products and services; to protect users of financial products and services from financially impaired or insolvent providers of such services; and to eliminate financial fraud, other criminal abuse and unethical conduct in the industry. Further, FSL Section 301 gives the Department broad power “to protect users of financial products and services.” In addition, FSL Section 302 provides the Department with equally broad authority to adopt regulations relating to “financial products and services,” which are broadly defined in the Financial Services Law to mean essentially any product or service offered by a Department-regulated entity. Accordingly, the Department has ample authority to adopt the proposed rule.

Other statutory authority includes: FSL Sections 202 and 408.

2. Legislative Objectives: The Financial Services Law is intended to ensure the safe and sound operation of the financial system. Cybercriminals present an ever-growing threat to that system. They can cause significant financial losses for Department-regulated entities and for New York consumers who use the products and services of those entities. In addition, the private information of such consumers may be revealed and/or stolen by cybercriminals for illicit purposes. The proposed rule is intended to ensure that all financial services providers regulated by the Department have and maintain cybersecurity programs that meet certain minimum cybersecurity standards in order to protect consumers and continue operating in a safe and sound manner.

3. Needs and Benefits: The proposed rule is necessary to ensure that Department-regulated entities are effectively addressing ever-growing cybersecurity risks in order to protect consumers and continue operating in a safe and sound manner.

4. Costs: All Department-regulated entities will be responsible for ensuring that they are in compliance with the proposed rule, which will impose some costs on their operations. The proposed rule provides for a limited exemption for certain smaller entities, based on each entity's number of employees, gross annual revenue, or year-end total assets. Entities that qualify for this limited exemption will be required to comply with only a limited number of sections in the proposed rule; thus, the costs of compliance for such entities is likely to be lower.

It is also anticipated that the costs of compliance will be offset to varying degrees when, as a result of complying with the proposed rule, entities avoid or mitigate cyber attacks that might otherwise have caused financial and other losses.

There should be no costs to any local governments as a result of the proposed rule.

5. Local government mandates: The proposed amendments do not impose any new programs, services, duties or responsibilities on local government.

6. Paperwork: The proposed rule requires entities to maintain a written cybersecurity policy and other written cybersecurity procedures and plans; to develop cybersecurity reports for presentation to the entity's board or a senior officer; to submit to the superintendent an annual certification of compliance with the proposed rule; and to keep books and records documenting compliance.

Entities that qualify for the limited exemption have fewer written policy and record-keeping requirements.

7. Duplication: Part 421 of Title 11 of the New York Codes, Rules and Regulations, promulgated in conformance with the federal Gramm-Leach-Bliley Act, requires insurance entities to implement a comprehensive written information security program. To a very limited extent, the proposed rule overlaps with Part 421, but the proposed rule includes requirements that are far more specific than Part 421 in order to achieve

more robust cybersecurity coverage and to ensure that the Department's regulated entities have and maintain cybersecurity programs that meet certain minimum cybersecurity standards in order to protect consumers and continue operating in a safe and sound manner. Notably, Section 6807(b) of the Gramm-Leach-Bliley Act allows states to implement a statute, regulation, order, or interpretation affording protections that are greater than those listed in the Gramm-Leach-Bliley Act.

8. Alternatives: None.

9. Federal Standards: As noted earlier, see "Duplication," above, the proposed rule will, in some respects, exceed minimum standards established by the federal Gramm-Leach-Bliley Act. The Department believes that the proposed rule is not inconsistent with the federal Gramm-Leach-Bliley Act. Indeed, the proposed rule includes requirements that are more specific than those in the federal Gramm-Leach-Bliley Act in order to achieve more robust cybersecurity coverage and to ensure that the Department's regulated entities protect consumers and continue operating in a safe and sound manner. Section 6807(b) of the Gramm-Leach-Bliley Act allows states to implement a statute, regulation, order, or interpretation affording protections that are greater than those listed in the Gramm-Leach-Bliley Act.

10. Compliance Schedule: Regulated entities will have 180 days from the effective date of the proposed rule to comply with its requirements, except as otherwise specified. The proposed rule will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the Superintendent a certification of compliance under Section 500.17 commencing February 15, 2018.

Regulatory Flexibility Analysis for Small Businesses and Local Governments for Proposed New 23 NYCRR 500.

1. Effect of the Rule: The proposed rule applies to all Department-regulated entities, but certain small businesses may qualify for a limited exemption provided for in Section 500.19 of the proposed rule. Those entities that qualify for the limited exemption – those that fall below the minimum specified number of employees, gross annual revenue, or year-end total assets – shall be exempt from the requirements of the proposed rule other than the requirements enumerated in Section 500.19.

The proposed rule does not apply to local governments and will not impose any adverse economic impact or any reporting, recordkeeping or other compliance requirements on local governments.

2. Compliance Requirements: Small businesses that do not qualify for the limited exemption found in Section 500.19 will be subject to all of the requirements of the proposed rule. If a small business does qualify for the limited exemption, such small business will be exempt from Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of the proposed rule.

3. Professional Services: A small business will not necessarily need any professional services to comply with the proposed rule. However, under the proposed rule, a Department-regulated entity that is a small business (or any other Department-regulated entity) that does not qualify for the limited exemption under Section 500.19 may use a third party service provider as its Chief Information Security Officer.

The proposed rule does not apply to local governments.

4. Compliance Costs: Like all businesses subject to the proposed rule, small businesses will be responsible for ensuring that they are in compliance with the proposed rule, which will impose some costs on their operations. The Department believes that the need for compliance outweighs such costs.

5. Economic and Technological Feasibility: The Department believes it will be economically and technologically feasible for small businesses to comply with the requirements of the proposed rule.

6. **Minimizing Adverse Impacts:** To minimize any adverse economic impact of the proposed rule on small businesses, the Department has included the limited exemption for smaller entities (Section 500.19 of the proposed rule). If a small businesses qualifies for the limited exemption, it will be subject to fewer compliance requirements.

7. **Small Business and Local Government Participation:** The proposed rule will be published publicly, including on the Department's website, for notice and comment, which will provide small businesses with the opportunity to participate in the rule making process.

The proposed rule does not impact local governments.

Statement as to why a revised Rural Area Flexibility Analysis (RAFA) is not required.

A revised Rural Area Flexibility Analysis (RAFA) is not required because the revisions to the proposed regulation do not change the conclusions set forth in the previously published RAFA.

Statement as to why a revised Job Impact Statement is not required.

A revised Job Impact Statement is not required because the revisions to the proposed regulation do not change the statement regarding the need for a Job Impact Statement that was previously published.