FREQUENTLY ASKED QUESTIONS REGARDING 23 NYCRR PART 500

Effective March 1, 2017, the Superintendent of Financial Services promulgated **23 NYCRR Part 500**, a regulation establishing cybersecurity requirements for financial services companies. The following provides answers to frequently asked questions concerning 23 NYCRR Part 500. Terms used below have the meanings assigned to them in 23 NYCRR 500.01. Please note that the Department may revise or update the below information from time to time, as appropriate.

1. **Assuming there is no continuous monitoring under 23 NYCRR Section 500.05, does the Department require that a Covered Entity complete a Penetration Test and vulnerability assessments by March 1, 2018?**

   The Regulation requires Covered Entities to have a plan in place that provides for Penetration Testing to be done as appropriate to address the risks of the Covered Entity. Such plan must encompass Penetration Testing at least annually and bi-annual vulnerability assessments, but the first annual Penetration Testing and first vulnerability assessment need not have been concluded before March 1, 2018 under Section 500.05. The Department expects all institutions with no continuous monitoring to complete robust Penetration Testing and vulnerability assessment in a timely manner as they are a crucial component of a cybersecurity program.

2. **If Covered Entity A utilizes Covered Entity B (not related to Covered Entity A) as a Third Party Service Provider, and Covered Entity B provides Covered Entity A with evidence of its Certification of Compliance with NYSDFS Cybersecurity Regulations, could that be considered adequate due diligence under the due diligence process required by Section 500.11(a)(3)?**

   No. The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider. Solely relying on the Certification of Compliance will not be adequate due diligence. Covered Entities must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks. The Department has provided a two year transitional period to address these risks and expects Covered Entities to have completed a thorough due diligence process on all Third Party Service Providers by March 1, 2019.

3. **Does a Covered Entity need 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))?**

   If there are changes, the Covered Entity should submit a new Notice of Exemption, which would not be considered an amendment to the original submission. For example, if a Covered Entity originally submitted a Notice of Exemption stating that it qualified for exemptions under Sections 500.19(b) and 500.19(a)(1), but it now only qualifies for a Section 500.19(a)(1) exemption, then the Covered Entity must submit a new Notice of Exemption with the correct information.

   The Department also emphasizes that Notices of Exemption should be filed electronically via the DFS Web Portal **http://www.dfs.ny.gov/about/cybersecurity**. The Covered Entity should utilize

the account that they used to file the original Notice of Exemption or create a new account if an individual filing was previously not made. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

4. **Should a Covered Entity send supporting documentation along with the Certification of Compliance?**

   The Covered Entity must submit the compliance certification to the Department and is not required to submit explanatory or additional materials with the certification. The certification is intended as a stand-alone document required by the regulation. The Department also expects that the Covered Entity maintains the documents and records necessary that support the certification, should the Department request such information in the future. Likewise, under 23 NYCRR Section 500.17, to the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity must document such efforts and maintain such schedules and documentation for inspection during the examination process or as otherwise requested by the Department.

5. **Is a Covered Entity entitled to an exemption under Section 500.19(b) if that Covered Entity is an employee, agent, representative or designee of more than one other Covered Entity?**

   Section 500.19(b) states that a Covered Entity who is an "employee, agent, representative or designee of a Covered Entity . . . is exempt from" 23 NYCRR Part 500 and "need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity" (emphasis added). This exemption requires an entire employee, agent, representative or designee to be fully covered by the program of another Covered Entity. Therefore, a Covered Entity who is an employee, agent, representative or designee of more than one other Covered Entity will only qualify for a Section 500.19(b) 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.

6. **Does a Covered Entity that qualifies for an exemption under 23 NYCRR Section 500.19(b) need to file a notice of exemption?**

   Yes. 23 NYCRR 500.19 subsections (a) through (d) set forth certain limited exemptions from different requirements of Part 500. Pursuant to 23 NYCRR Section 500.19(e): "[a] Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption" (emphasis added).

7. **Under Section 500.04(b), can the requirement that the CISO report in writing at least annually "to the Covered Entity's board of directors" (the "board") be met by reporting to an authorized subcommittee of the board?**

No. The Department emphasizes that a well-informed board is a crucial part of an effective cybersecurity program and the CISO's reporting to the full board is important to enable the board to assess the Covered Entity's governance, funding, structure and effectiveness as well as compliance with 23 NYCRR Part 500 or other applicable laws or regulations.

8. **Can a Covered Entity file a notice of exemption on behalf of its employees or agents?**

   By permission, the Department will approve certain Covered Entities to file notices of exemption on behalf of their employees or captive agents who are also Covered Entities. This option will only be available for filings of 50 or more employees or captive agents and only if all employees or captive agents qualify for the same exemptions. Covered Entities with over 50 employees or agents on whose behalf they have authority to file should contact the Department at **CyberRegComments@dfs.ny.gov** from the email to which your Cybersecurity portal account is associated with the **following instructions**. The Department will coordinate with the Covered Entity to submit a one-time filing form to effectuate an exemption filing for multiple covered entities. On the spreadsheet, the submitter will need to provide the first and last name, DFS identification number, type of license, and email for every employee or captive agent. After approval, the Department will send more detailed instructions and the exemption spreadsheet. In the event that there is a need for additional names or captive agents after the initial submission, the submitter will be able to submit a supplemental form through the portal. The Department emphasizes that the employee or captive agent, for whom the Covered Entity is filing, continues to be ultimately responsible in ensuring compliance with 23 NYCRR Part 500. It remains the responsibility of the employee or captive agent to notify the Department of any changes in their status.

9. **When is an unsuccessful attack a Cybersecurity Event that has or had "a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity" under the reporting requirements of 23 NYCRR Section 500.17(a)(2)?**

   The Department recognizes that Covered Entities are regularly subject to many attempts to gain unauthorized access to, disrupt or misuse Information Systems and the information stored on them, and that many of these attempts are thwarted by the Covered Entities' cybersecurity programs. The Department anticipates that most unsuccessful attacks will *not* be reportable, but seeks the reporting of those unsuccessful attacks that, in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern. For example, notice to the Department under 23 NYCRR Section 500.17(a)(2) would generally *not* be required if, consistent with its Risk Assessment, a Covered Entity makes a good faith judgment that the unsuccessful attack was of a routine nature.

   The Department believes that analysis of unsuccessful threats is critically important to the ongoing development and improvement of cybersecurity programs, and

Covered Entities are encouraged to continually develop their threat assessment programs. Notice of the especially serious unsuccessful attacks may be useful to the Department in carrying out its broader supervisory responsibilities, and the knowledge shared through such notice can be used to timely improve cybersecurity generally across the industries regulated by the Department. Accordingly, Covered Entities are requested to notify the Department of those unsuccessful attacks that appear particularly significant based on the Covered Entity's understanding of the risks it faces. For example, in making a judgment as to whether a particular unsuccessful attack should be reported, a Covered Entity might consider whether handling the attack required measures or resources well beyond those ordinarily used by the Covered Entity, like exceptional attention by senior personnel or the adoption of extraordinary non-routine precautionary steps.

The Department recognizes that Covered Entities' focus should be on preventing cybersecurity attacks and improving systems to protect the institution and its customers. The Department's notice requirement is intended to facilitate information sharing about serious events that threaten an institution's integrity and that may be relevant to the Department's overall supervision of the financial services industries. The Department trusts that Covered Entities will exercise appropriate judgment as to which unsuccessful attacks must be reported and does not intend to penalize Covered Entities for the exercise of honest, good faith judgment.

10. **Are the New York branches of out-of-state domestic banks required to comply with 23 NYCRR Part 500?**

New York is a signatory to the Nationwide Cooperative Agreement, Revised as of December 9, 1997 (the "Agreement"), an agreement among state banking regulators that addresses supervision in an interstate branching environment. Pursuant to the Agreement, the home state of a state-chartered bank with a branch or branches in New York under Article V-C of the New York Banking Law is primarily responsible for supervising such state-chartered bank, including its New York branches. In keeping with the Agreement's goals of interstate coordination and cooperation with respect to the supervision and examination of bank branches, including compliance with applicable laws, DFS will defer to the home state supervisor for supervision and examination of the New York branches, with the understanding that DFS is available to coordinate and work with the home state in such supervision and examination. DFS notes that New York branches are required to comply with New York state law, and DFS maintains the right to examine branches located in New York. With respect to DFS's cybersecurity regulation, given the ever-increasing cybersecurity risks that financial institutions face, DFS strongly encourages all financial institutions, including New York branches of out-of-state domestic banks, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500.

11. **How must a Covered Entity address cybersecurity issues with respect to its subsidiaries and other affiliates?**

    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 (see 23 NYCRR Sections 500.09, 500.02 and 500.03, respectively). Other regulatory requirements may also apply, depending on the individual facts and circumstances.

12. **If a Covered Entity qualifies for a limited exemption, does it need to comply with 23 NYCRR Part 500?**

    The exemptions listed in 23 NYCRR Part 500.19 are limited in scope. These exemptions have been tailored to address particular circumstances and include requirements that the Department believes are necessary for these exempted entities. As such, Covered Entities that qualify for those exemptions are only exempt from complying with certain provisions as set forth in the regulation, but must comply with the sections listed in the exemption that applies to that Covered Entity.

13. **Under 23 NYCRR 500.17(a), is a Covered Entity required to give notice to the Department when a Cybersecurity Event involves harm to consumers?**

    Yes. 23 NYCRR 500.17(a) must be read in combination with other laws and regulations that apply to consumer privacy. Under 23 NYCRR 500.17(a)(1), a Covered Entity must give notice to the Department of any Cybersecurity Event "of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body," which includes many Cybersecurity Events that involve consumer harm, whether actual or potential. To offer just one example, New York's information security breach and notification law requires notices to affected consumers and to certain government bodies following a data breach. Under 23 NYCRR 500.17(a)(1), when such a data breach constitutes a Cybersecurity Event, it must also be reported to the Department.

    In addition, under 23 NYCRR 500.17(a)(2), Cybersecurity Events must be reported to the Department if they "have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." To the extent a Cybersecurity Event involves material consumer harm, it is covered by this provision.

14. **Is a Covered Entity required to give notice to consumers affected by a Cybersecurity Event?**

    New York's information security breach and notification law (General Business Law Section 899-aa), requires notice to consumers who have been affected by cybersecurity incidents. Further, under 23 NYCRR Part 500, a Covered Entity's cybersecurity program and policy must address, to the extent applicable, consumer data privacy and other consumer protection issues. Additionally, Part 500 requires that Covered Entities address as part of their incident response plans external

communications in the aftermath of a breach, which includes communication with affected customers. Thus, a Covered Entity's cybersecurity program and policies will need to address notice to consumers in order to be consistent with the risk-based requirements of 23 NYCRR Part 500.

15. **May a Covered Entity adopt portions of an Affiliate's cybersecurity program without adopting all of it?**

    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 23 NYCRR Part 500. The Covered Entity remains responsible for full compliance with the requirements of 23 NYCRR Part 500. To the extent a Covered Entity relies on an Affiliate's cybersecurity program in whole or in part, that program must be made available for examination by the Department.

16. **May the certification requirement of 23 NYCRR 500.17(b) be met by an Affiliate?**

    No. Each Covered Entity is required to annually certify its compliance with Part 500 as required by 23 NYCRR 500.17(b).

17. **To the extent a Covered Entity uses an employee of an Affiliate as its Chief Information Security Officer ("CISO"), is the Covered Entity required to satisfy the requirements of 23 NYCRR 500.04(a)(2)-(3)?**

    To the extent a Covered Entity utilizes an employee of an Affiliate to serve as the Covered Entity's CISO for purposes of 23 NYCRR 500.04(a), the Affiliate is not considered a Third Party Service Provider for purposes of 23 NYCRR 500.04(a)(2)-(3). However, the Covered Entity retains full responsibility for compliance with the requirements of 23 NYCRR Part 500 at all times, including ensuring that the CISO responsible for the Covered Entity is performing the duties consistent with this Part.

18. **Are the DFS-authorized New York branches, agencies and representative offices of out-of-country foreign banks required to comply with 23 NYCRR Part 500?**

    Yes. It is further noted that, in such cases, only the Information Systems supporting the branch, agency or representative office, and the Nonpublic Information of the branch, agency or representative office are subject to the applicable requirements of 23 NYCRR Part 500, whether through the branch's, agency's or representative office's development and implementation of its own cybersecurity program or through the adoption of an Affiliate's cybersecurity program.

19. **Where interrelated requirements under 23 NYCRR Part 500 are subject to different transitional periods, when and to what extent are Covered Entities required to comply with currently applicable requirements that are impacted by separate requirements for which the applicable transitional period has not yet ended?**

    Covered Entities have 180 days from the March 1, 2017, effective date to come into compliance with the requirements of 23 NYCRR Part 500 unless otherwise specified in 23 NYCRR 500.22. While complying with currently applicable requirements under the

final rule, Covered Entities are generally not required to comply with, or incorporate into their cybersecurity programs, provisions of the regulation for which the applicable transitional period has not yet ended. For example, while Covered Entities will be required to have a cybersecurity program as well as policies and procedures in place by August 28, 2017, the Department recognizes that in some cases there may be updates and revisions thereafter that incorporate the results of a Risk Assessment later conducted, or other elements of Part 500 that are subject to longer transitional periods.

20. **Is a Covered Entity required to certify compliance with all the requirements of 23 NYCRR 500 on February 15, 2018?**

    Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) by February 15, 2018. This initial certification applies to and includes all requirements of 23 NYCRR Part 500 for which the applicable transitional period under 23 NYCRR 500.22 has terminated prior to February 15, 2018. Accordingly, Covered Entities will not be required to submit certification of compliance with the requirements of 23 NYCRR 500.04(b), 500.05, 500.06, 500.08, 500.09, 500.12, 500.13, 500.14 and 500.15 until February 15, 2019, and certification of compliance with 23 NYCRR 500.11 until February 15, 2020.

21. **May a Covered Entity submit a certification under 23 NYCRR 500.17(b) if it is not yet in compliance with all applicable requirements of Part 500?**

    The Department expects full compliance with this regulation. A Covered Entity may not submit a certification under 23 NYCRR 500.17(b) unless the Covered Entity is in compliance with all applicable requirements of Part 500 at the time of certification. To the extent a particular requirement of Part 500 is subject to an ongoing transitional period under 23 NYCRR 500.22 at the time of certification, that requirement would not be consider applicable for purposes of a certification under 23 NYCRR 500.17(b).

22. **What constitutes "continuous monitoring" for purposes of 23 NYCRR 500.05?**

    Effective continuous monitoring could be attained through a variety of technical and procedural tools, controls and systems. There is no specific technology that is required to be used in order to have an effective continuous monitoring 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 may 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 to constitute "effective continuous monitoring" for purposes of 23 NYCRR 500.05.

23. **When is a Covered Entity required to report a Cybersecurity Event under 23 NYCRR 500.17(a)?**

23 NYCRR 500.17(a) requires Covered Entities to notify the superintendent of certain Cybersecurity Events as promptly as possible but in no event later than 72 hours from a determination that a reportable Cybersecurity Event has occurred. A Cybersecurity Event is reportable if it falls into at least one of the following categories:

- the Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- the Cybersecurity Event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

An attack on a Covered Entity may constitute a reportable Cybersecurity Event even if the attack is not successful.

24. **How should a Covered Entity submit Notices of Exemption, Certifications of Compliance and Notices of Cybersecurity Events?**

    Cybersecurity Notices of Exemption, Certifications of Compliance, and Notices of Cybersecurity Events should be filed electronically via the DFS Web Portal **http://www.dfs.ny.gov/about/cybersecurity**. You will first be prompted to create an account and log in to the DFS Web Portal, then directed to the filing interface. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

25. **Can an entity be both a Covered Entity and a Third Party Service Provider under 23 NYCRR Part 500?**

    Yes. If an entity is both a Covered Entity and a Third Party Service Provider, the entity is responsible for meeting the requirements of 23 NYCRR Part 500 as a Covered Entity.

26. **Are all Third Party Service Providers required to implement Multi-Factor Authentication and encryption when dealing with a Covered Entity?**

    23 NYCRR 500.11, among other things, generally requires a Covered Entity to develop and implement written policies and procedures designed to ensure the security of the Covered Entity's Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. 23 NYCRR 500.11(b) requires a Covered Entity to include in those policies and procedures guidelines, as applicable, addressing certain enumerated issues. Accordingly, 23 NYCRR 500.11(b) requires Covered Entities to make a risk assessment regarding the appropriate controls for Third Party Service Providers based on the individual facts and circumstances presented and does not create a one-size-fits-all solution.