Q&A

During and following our roundtable presentation on April 5, 2017 on the New York Department of Financial Services (DFS) cybersecurity regulations, we were grateful to receive so many thoughtful questions from participants. As a follow-up to our presentation, we thought it would be helpful to provide general responses to your questions in a Q&A format, which we offer below. If you have any further questions about the topics discussed at the roundtable or in this Q&A, please contact your Morgan Lewis lawyer or any of the contacts listed at the end of the document.

Please note—unless otherwise defined herein, all defined terms (e.g., Covered Entity, Information System, Nonpublic Information) correlate to the terms as defined in the DFS cybersecurity regulations.

Question	While the risk assessment is not required until March 1, 2018, why is it important for compliance with the regulations as a whole?
Response	The risk assessment is a cornerstone for many of the DFS cybersecurity requirements—including the required cybersecurity program and policies—and it should be started or reviewed immediately to timely and appropriately design and implement a Covered Entity's cybersecurity program and other required activities under the regulations.
Question	As a Covered Entity, do I need to hire a Chief Information Security Officer (CISO)? Do I need to hire other employees to be compliant with the rules?
Response	A Covered Entity does not need to hire or otherwise designate a person with the formal "CISO" title. However, a Covered Entity must designate a "qualified individual" responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. A Covered Entity may designate a qualified individual who is employed by the Covered Entity itself or by an affiliate or third party service provider. If the qualified individual is not employed by the Covered Entity, the Covered Entity is still responsible for compliance with the DFS cybersecurity rules. (*See* Section 500.04)

	In addition, a Covered Entity must use qualified cybersecurity personnel to manage its cybersecurity risks and perform or oversee the performance of the cybersecurity program's core functions. Such personnel can be employed by the Covered Entity, an affiliate, or a third party service provider. Also, a Covered Entity can use an affiliate or qualified third party service provider to assist in compliance with the DFS cybersecurity requirements. A Covered Entity should determine who will serve as its qualified cybersecurity personnel or how it will otherwise fulfill the requirements of the DFS cybersecurity rules. Although it is not necessary to hire new personnel, a gap analysis may demonstrate areas where a Covered Entity may need to retain personnel to fulfill core cybersecurity functions, and could retain such personnel from an affiliate or third party service provider. (*See* Section 500.10)
Question	Do the rules cover only personal information pertaining to customers or do they cover a broader scope of information?
Response	The DFS cybersecurity rules cover a broad scope of information, including the types of information typically considered to be personally identifiable information related to individual customers, as well as trade secrets and other business-related information that is not publicly available. The DFS cybersecurity rules require a Covered Entity to maintain a cybersecurity program designed to identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on its Information Systems (*see* Section 500.02(b)(1)). The rules include a definition of "Nonpublic Information," which encompasses electronic information that is not publicly available and falls into any of the following categories: • *Business related information* of a Covered Entity, the tampering with which or the unauthorized disclosure, access, or use of which would cause a *material adverse impact to the business, operations, or security* of the Covered Entity. • Any *information concerning an individual* that—because of name, number, personal mark, or other identifier—can be used to identify such individual in combination with any one or more of the following data elements: o Social Security number o Driver's license number or non-driver identification card number o Account number or credit or debit card number o Any security code, access code, or password that would permit access to an individual's financial account o Biometric records • Any information or data, except age or gender, in any form or medium created by or derived from a healthcare provider or an individual and that relates to o the past, present, or future physical, mental, or behavioral health or condition *of any individual or a member of the individual's family*; o the provision of healthcare to *any individual*; or o payment for the provision of healthcare to *any individual*.
Question	When should I start adding representations about cybersecurity in my third party services

	agreements?
Response	A Covered Entity should begin considering now how it will incorporate, in its agreements with third party service providers, representations covering their cybersecurity policies and procedures—including those related to access controls, use of multi-factor authentication, encryption, and notice of certain Cybersecurity Events. The reason a Covered Entity should consider its approach to third party service provider agreements sooner rather than later is to allow adequate time to review and, if necessary, modify relevant agreements by the March 1, 2019 compliance date.
Question	Are there steps that Covered Entities should start taking now to prepare for the annual compliance certification's February 15, 2018 compliance date?
Response	A Covered Entity's board of directors or the equivalent senior management or governing body (for our purposes, the "board") should evaluate the types of reports or information the board needs to receive in order to make the certification. Appropriate personnel should begin preparing such reports or compiling relevant information in advance of the February 15, 2018 deadline for making the first annual compliance certification. Beginning on March 1, 2018, the individual responsible for performing "CISO" duties is required to provide to the board with an annual written report on, among other things, material cybersecurity risks and the overall effectiveness of the Covered Entity's cybersecurity program. Despite the later compliance date, a board may find this type of report useful in making the annual compliance certification. The board and the individual responsible for the CISO annual report should consider whether the annual report should be submitted to the board ahead of its compliance date for purposes of providing the board with relevant information to consider when making the annual compliance certification.
Question	Are licensed insurance agencies in New York subject to this regulation?
Response	We interpret "licensed insurance agencies in New York" to mean insurance agencies operating pursuant to a DFS-issued license. Accordingly, such insurance agencies are subject to the DFS cybersecurity rules unless an exemption applies (as described below). Even if an insurance agency is "exempt," it likely will be required to comply with a portion of the rules. Exemptions that could be applicable to a licensed insurance agency include the following: 1. Small Covered Entity exemptions: o "Fewer than 10 employees" located in New York or responsible for the Covered Entity's business (*see* Section 500.19(a)(1)). o "Gross Revenue Test"—less than $5 million in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates (*see* Section 500.19(a)(2)). o "Year-End Total Assets Test"—less than $10 million in year-end total assets, calculated in accordance with Generally Accepted Accounting Principles (GAAP), including assets of all Affiliates (*see* Section 500.19(a)(3)). Under these exemptions, a Covered Entity is exempt from Sections 500.04, 05, 06, 08, 10, 12, 14, 15, and 16. 2. Section 500.19(c) provides an exemption for a firm "that does not directly or

	indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information." Under this exemption, a Covered Entity is exempt from Sections 500.02, 03, 04, 05, 06, 07, 08, 10, 12, 14, 15, and 16. 3. Captive Insurance Companies (*see* Section 500.19(d))—see below for more information about this exemption. 4. Charitable Annuity Societies (*see* Section 1110 of the Insurance Law), risk retention groups (*see* Section 5904 of the Insurance Law), and accredited reinsurers or certified reinsurers that have been accredited or certified (*see* 11 NYCRR 125) are fully exempt from the DFS cybersecurity rules (*see* Section 500.19(f)).
Question	Are health insurance companies without financial services covered?
Response	If the health insurer operates in New York under a license or authorization granted by the DFS under the New York Insurance Law, it is subject to the DFS cybersecurity regulations (unless an exemption applies). The definition of "Nonpublic Information" captures a broad array of business and personal (including health-related) information. As described above, Nonpublic Information includes information relating to the past, present, or future physical, mental, or behavioral health or condition of any individual or a member of the individual's family; the provision of healthcare to any individual; or payment for the provision of healthcare to any individual.
Question	Do these regulations apply to a broker-dealer not affiliated with a bank or insurance company or other covered party?
Response	A broker-dealer that does not have a DFS-issued license, registration, charter, certificate, permit, accreditation, or similar authorization under the Banking Law, Insurance Law, or Financial Services Law does not fall within the scope of a "Covered Entity" and therefore is not subject to the DFS cybersecurity rules. It is our view that a broker-dealer generally would not fall within the scope of the rules unless it is affiliated with a Covered Entity and both entities share Information Systems. To the extent that a broker-dealer provides third party services to Covered Entities, the broker-dealer's Covered Entity clients may require the broker-dealer to provide appropriate assurances or warranties about the broker-dealer's cybersecurity program or otherwise ask to renegotiate existing service agreements.
Question	Is a New York-licensed health insurance agency located in New York with licensed agents throughout the country subject to the rule and considered a Covered Entity?
Response	Yes, a health insurance agency operating in New York pursuant to a DFS-issued license is a "Covered Entity," but it should determine whether it can rely on any exemption(s). Still, to the extent that the cybersecurity rules apply to the health insurance agency, agents (or other employees or contractors) outside of New York could be deemed "Authorized Users" if they are authorized to access and use any Information Systems and data of the New York-authorized health insurance agency. Thus, it would be prudent to inventory which personnel have access to such Information Systems to determine the scope of application of the

	requisite cybersecurity program under DFS rules.
Question	How do the regulations impact independent insurance agents and agencies? Is it sufficient to apply the rules at the agency level or should they be applied as far down as the independent agent level?
Response	Independent insurance agents and agencies licensed by DFS are "Covered Entities." In turn, Section 500.19(b) provides an exemption from the requirement to develop a cybersecurity program to an employee, agent, representative, or designee of a Covered Entity that is itself a Covered Entity. Pursuant to this exemption, such employee, agent, representative, or designee may rely on the agency-level cybersecurity program—provided that it is covered by the agency's cybersecurity program.
Question	Can you reiterate the scope of the rules as they apply to captive insurers, including Bermuda-based captive insurers? My understanding is that captives are covered if they provide third party coverage beyond those provided to the parent.
Response	A captive insurance company that is approved under Article 70 of the Insurance Law (regardless of its jurisdiction of domicile) falls within an exemption from the rules pursuant to Section 500.19(d) if the captive insurance company "does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates)." However, this exemption is not a blanket exemption. The captive insurance company is subject to Sections 500.09 (Risk Assessment), 11 (Third Party Service Provider Security Policy), 13 (Limitations on Data Retention), 17 (Notices to Superintendent), 18 (Confidentiality), 19 (Exemptions), and 20 (Enforcement). To rely on an exemption, the captive insurance company must submit to DFS a notice of exemption in the format provided in Appendix B to the DFS cybersecurity rules. A captive insurance company falls within the scope of the rules in their entirety if it directly or indirectly controls, owns, accesses, generates, receives, or possesses Nonpublic Information other than that relating to its parent company or an Affiliate. However, to the extent that another exemption applies to the captive insurance company, it could rely on the other exemption.

Contacts

If you have any questions or would like more information on the issues discussed in this Q&A, please contact any of the following Morgan Lewis lawyers:

Washington, DC
Charles Horn
Melissa Hall

Silicon Valley
Mark L. Krotoski

Chicago
Sarah V. Riddell