August 9, 2017

# NYSDFS Upcoming Deadline Fast Approaching: First Key Date is August 28, 2017

Authors:

Stephen M. Forte
(212) 376-3015
sforte@goodwin.com

Michael T. Conway
(212) 376-3011
mconway@goodwin.com

On March 1, 2017, the New York State Department of Financial Services' ("DFS") first-in-nation Cybersecurity Regulations for the purpose of protecting consumers and financial institutions from cyber-attacks went into effect (the "Regulations"). See, 23 NYCRR Part 500. The "first-in-nation" nature of the Regulations is extremely important to note because the Regulations apply not only to what is referred to in the Regulations as a "Covered Entity" based in New York, but also those that merely do business in New York. The Regulations also do not just cover financial institutions, but any business entity that is covered by the banking law, insurance law, or financial services laws. A brief overview of who is covered, key dates, and the areas with which compliance must be met by August 28, 2017 is below.

**Who is a Covered Entity:**

With the exception of an "Exempted Entity" (see below), the Regulations apply to any entity or organization "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization" pursuant to New York banking law, insurance law, or financial services laws. This may include New York-licensed lenders, mortgage banks, life insurance companies, savings and loans, charitable foundations and other financial services firms, among others. If your business transacts business in the State of New York, it is important to verify whether your business qualifies as a Covered Entity.

**Who is an Exempt Entity:**

Not all Covered Entities are required to comply with the Regulations in their entirety. Those with less than 10 employees or independent contractors, less than $5 million in gross annual revenue in each of the last three fiscal years, or less than $10 million in year-end total assets are exempt and do not need to comply with sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15 and 500.16. These Regulations also do not apply to national banks, federal savings banks, and federally chartered branches of non-U.S. banks (because these entities are regulated by federal law, not New York State law), but will apply to New York chartered or licensed lenders and New York branches of foreign banks. It should be noted that a parent, affiliate or subsidiary of an Exempt Entity that does not have its own basis for an exemption cannot rely on the fact that its parent, affiliate or subsidiary is an Exempt Entity. Therefore, Regulations may still indirectly impact national banks, federal savings banks, and federally-chartered branches of non-U.S. banks. Additional exemptions may also apply under section 500.19. Even exempt entities should be cognizant of the Regulations and requirements thereunder as a standard for protecting third-party information.

## Key Dates:

Although the Regulations were effective March 1, 2017, there are several key dates that all Covered Entities should be aware of regarding compliance: Those dates, and the relevance of those dates, are as follows:

- **August 28, 2017:** The 180-day transitional period afforded by the Regulation from its effective date ends. Unless otherwise specified, this is that date by which all Covered Entities are required to be in compliance with the Regulations, unless otherwise stated in 23 NYCRR 500.22 or if the applicable transitional period has not yet expired.

- **September 27, 2017:** 23 NYCRR 500.19(e) provides for a thirty-day period for a Covered Entity to file a Notice of Exemption. By September 27, 2017, Covered Entities will need to have determined whether as of August 28, 2017 they qualified for a limited exemption under 23 NYCRR 500.19(a) - (d).

- **February 15, 2018:** First certification is required to be submitted by Covered Entities pursuant to 23 NYCRR 500.17(b) on or before this date. A certification of compliance is not yet required for 23 NYCRR 500.04(b), 500.06, 500.08, 500.09, 500.11, 500.12, 500.13, 500.14 or 500.15.

- **March 1, 2018:** The one-year transitional period afforded by the Regulation from its effective date ends. Unless otherwise specified, this is that date by which all Covered Entities are required to be in compliance with section 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of the Regulations.

- **September 3, 2018:** The eighteen-month transitional period afforded by the Regulation from its effective date ends. Unless otherwise specified, this is that date by which all Covered Entities are required to be in compliance with section 500.06, 500.08, 500.13, 500.14(a), and 500.15 of the Regulations.

- **March 1, 2019:** Two-year transitional period afforded by the Regulations from its effective date expires. Unless otherwise specified, this is the date by which all Covered Entities must be in compliance with section 500.11 of the Regulations.

## What is Required by August 28, 2017:

A brief breakdown of what is required under each subsection of the Regulations for which compliance is required by August 28, 2017 is below:

**Section 500.02:** Cybersecurity program must be maintained based on the Risk Assessment for the purpose of protecting the “confidentiality, integrity and availability of the Covered Entity’s Information System.”

**Section 500.03:** A written Cybersecuirty Policy must be implemented and maintained based on the Risk Assessment setting forth the policies and procedures for the protection of Information Systems and Nonpublic Information stored on the Information Systems. The Regulation also enumerates 14 specific areas that should be addressed in the Cybersecurity Policy.

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

265 Church Street - Suite 1207
New Haven, CT 06510-7013
203-836-2801

400 Park Avenue - Fifth Floor
New York, NY 10022-4406
212-376-3010

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

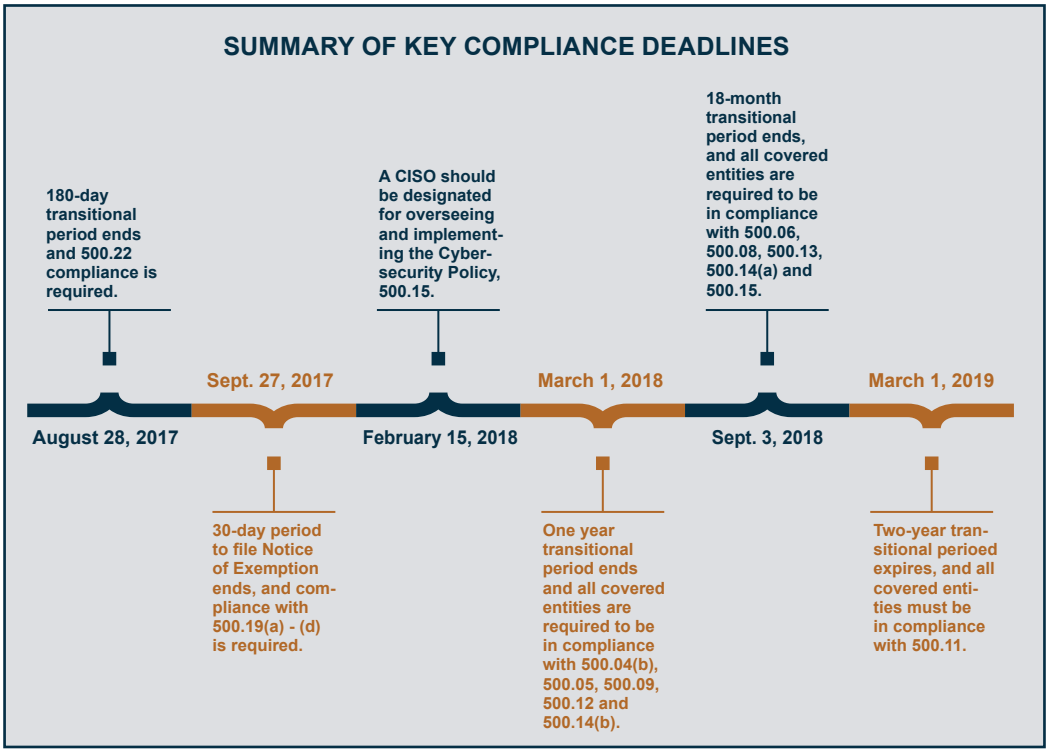
1875 K St., NW - Suite 600
Washington, DC 20006-1251
202-469-7750

www.shipmangoodwin.com

**Section 500.04:** A Chief Information Security Officer ("CISO") should be designated (either internally, through an affiliate or through a third-party service provider). The CISO will be the individual made responsible for overseeing and implementing the Cybersecurity Policy. Notably, a Section 500.04(b) requires the CISO to issue a report on an at least annual basis. As such, compliance with subsection (b) is not required until March 1, 2018 – a year after the enactment of the Regulations.

**Section 500.07:** Access privileges to Information Systems that provide access to Nonpublic Information must be limited. As part of this subsection, a periodic review of access privileges should be conducted.

**Section 500.16:** A written incident response plan must be created. The Incident Response Plan must specifically seven areas as set forth in the Regulations.




With the first key compliance deadline fast approaching, it is important that your company ensures the necessary steps for compliance have been met and that the reporting deadline is calendared. We will continue to provide updates as dates approach.

## Questions or Information:

For more information on New York's Cybersecurity regulations, please contact Stephen Forte at (212) 376-3015 or sforte@goodwin.com or Michael Conway at (212) 376-3011 or mconway@goodwin.com.



SHIPMAN & GOODWIN LLP®
COUNSELORS AT LAW