Client Alert | Financial Institutions Advisory

NYDFS Cybersecurity Regulations Compliance Guide: Applicability, Exemptions and Penalties

March 2017

Authors: Steven Chabinsky, Kevin Petrasic, Helen Lee

As discussed in our March 1, 2017 update,[1] the New York Department of Financial Services ("NYDFS") issued final regulations that require New York banks and insurance companies, as well as other financial services companies that are supervised by the NYDFS—including New York state-licensed branches and agencies of non-US banks—to establish and maintain a cybersecurity program designed to protect consumers' private data and ensure the safety and soundness of New York's financial services industry ("Cybersecurity Regulations").[2] The Cybersecurity Regulations are contained in new Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, 23 NYCRR 500, and are available here.

The Cybersecurity Regulations took effect on March 1, 2017, but are subject to a 180-day transitional period (i.e., until August 28, 2017) for general compliance. Additional transitional periods are provided for specific provisions of the Cybersecurity Regulations. Covered Entities (defined below) will be required annually to prepare and submit to the NYDFS Superintendent a Certification of Compliance with the Cybersecurity Regulations commencing February 15, 2018.

Overview

In recognition of the growing nature of cyberthreats facing US financial institutions, including those supervised by the NYDFS, the NYDFS issued the Cybersecurity Regulations to promote the protection of customer information as well as the information technology systems of supervised entities.

Financial Institutions Advisory

Bank Advisory
Broker-Dealer
Consumer Financial Services
Cybercurrency
Cybersecurity
Data Privacy & Protection
EU and WTO
FinTech
Investment Advisory & Management
Payments
Sanctions, Bank Secrecy and Export Controls
Securities
Trust and Fiduciary

In general, the regulations require supervised entities to assess their specific risk profile and design a program that addresses cybersecurity risks in a robust fashion. As detailed more fully in our March 1 **update**, the Cybersecurity Regulations impose certain regulatory minimum standards aimed at helping institutions to prevent and avoid cyber breaches. Such minimum standards include:

- Controls relating to the governance framework for a robust cybersecurity program including requirements for a program that is adequately funded and staffed, overseen by qualified management, and reported on periodically to the most senior governing body of the organization;
- Risk-based minimum standards for technology systems including access controls, data protection including encryption, and penetration testing, to be achieved under a risk assessment which, as stated by NYDFS, is not intended to permit a cost-benefit analysis of acceptable losses where an institution is faced with cybersecurity risks;
- Required minimum standards to help address any cyber breaches including an incident response plan, preservation of data to respond to such breaches, and notice to the NYDFS of material events; and
- Accountability by requiring identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance to the NYDFS.

Applicability and Exemptions

The Cybersecurity Regulations apply to all individuals and entities (including branches and agencies of non-US banks) operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York Banking Law, the New York Insurance Law or the New York Financial Services Law (each, a "Covered Entity").

The Cybersecurity Regulations provide for nine *types* of entities that fall under five *categories* of exemptions. Importantly, most of the exemptions are limited, in that they only provide compliance relief for certain sections of the Cybersecurity Regulations. Accordingly, exempt Covered Entities should take care to determine which cybersecurity obligations remain relevant to the Covered Entity notwithstanding the availability of an exemption. The exemptions and relevant compliance obligations are set forth in table format in **Appendix A** attached.

NOTICE REQUIREMENT**:** Except as noted below, a Covered Entity that qualifies for an exemption is required to file a Notice of Exemption in the form set forth in Appendix B to the Cybersecurity Regulations within 30 days of the determination that the Covered Entity is exempt.

CHANGE IN STATUS: If a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, it has 180 days from the fiscal year end to comply with all applicable requirements.

Exemption Category 1: Small Covered Entities

- **Exemption Type 1:** Covered Entities with fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates[3] located in New York or responsible for business of the Covered Entity (Section 500.19(a)(1));
- **Exemption Type 2:** Covered Entities with less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates (Section 500.19(a)(2)); and
- **Exemption Type 3:** Covered Entities with less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates (Section 500.19(a)(3)).

Covered Entities under exemption Category 1 are exempt from requirements under sections 500.04 (Chief Information Security Officer), 500.05 (Penetration Testing and Vulnerability Assessments), 500.06 (Audit Trail),

500.08 (Application Security), 500.10 (Cybersecurity Personnel and Intelligence), 500.12 (Multi-Factor Authentication), 500.14 (Training and Monitoring), 500.15 (Encryption of Nonpublic Information), and 500.16 (Incident Response Plan) of the Cybersecurity Regulations.

Importantly, Covered Entities under exemption Category 1 continue to be subject to compliance obligations under sections 500.02 (Cybersecurity Program), 500.03 (Cybersecurity Policy), 500.07 (Access Privileges), 500.09 (Risk Assessment), 500.11 (Third Party Service Provider Security Policy), 500.13 (Limitations on Data Retention), and 500.17 (Notices to Superintendent) of the Cybersecurity Regulations. Covered Entities under this category are required to file a Notice of Exemption in the form set forth in Appendix B to the Cybersecurity Regulations within 30 days of the determination that the Covered Entity is exempt.

Exemption Category 2: Employees, Agents, Representatives and Designees

- **Exemption Type 4:** Employees, agents, representatives or designees of a Covered Entity who are covered by the cybersecurity program of the Covered Entity. (Section 500.19(b)).

The definition of Covered Entity is broad and includes both individuals and non-governmental entities subject to the jurisdiction of the NYDFS. As a result, employees and other representatives of Covered Entities may also themselves meet the definition of a Covered Entity. Covered Entities under exemption Category 2 are exempt from the substantive requirements of the Cybersecurity Regulations (except the notice requirement) and need not develop their own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity. Covered Entities under this category are required to file a Notice of Exemption in the form set forth in Appendix B to the Cybersecurity Regulations within 30 days of the determination that the Covered Entity is exempt.

Exemption Category 3: Covered Entities without Access to Information Systems or Nonpublic Information

- **Exemption Type 5:** Covered Entities that do not directly or indirectly operate, maintain, utilize or control any Information Systems,[4] and that do not, and are not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information.[5] (Section 500.19(c)).

Covered Entities under exemption Category 3 are exempt from the requirements of sections 500.02 (Cybersecurity Program), 500.03 (Cybersecurity Policy), 500.04 (Chief Information Security Officer), 500.05 (Penetration Testing and Vulnerability Assessments), 500.06 (Audit Trail), 500.07 (Access Privileges), 500.08 (Application Security), 500.10 (Cybersecurity Personnel and Intelligence), 500.12 (Multi-Factor Authentication), 500.14 (Training and Monitoring), 500.15 (Encryption of Nonpublic Information), and 500.16 (Incident Response Plan) of the Cybersecurity Regulations.

Importantly, Covered Entities under exemption Category 3 continue to be subject to compliance obligations under sections 500.09 (Risk Assessment), 500.11 (Third Party Service Provider Security Policy), 500.13 (Limitations on Data Retention), and 500.17 (Notices to Superintendent) of the Cybersecurity Regulations. Covered Entities under this category are required to file a Notice of Exemption in the form set forth in Appendix B to the Cybersecurity Regulations within 30 days of the determination that the Covered Entity is exempt.

Exemption Category 4: Insurance Covered Entities without Access to Nonaffiliate Nonpublic Information

- **Exemption Type 6:** Covered Entities under Article 70 of the Insurance Law that do not and are 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). (Section 500.19(d)).

Covered Entities under exemption Category 4 are exempt from the requirements of sections 500.02 (Cybersecurity Program), 500.03 (Cybersecurity Policy), 500.04 (Chief Information Security Officer), 500.05 (Penetration Testing and Vulnerability Assessments), 500.06 (Audit Trail), 500.07 (Access Privileges), 500.08 (Application Security), 500.10 (Cybersecurity Personnel and Intelligence), 500.12 (Multi-Factor Authentication), 500.14 (Training and Monitoring), 500.15 (Encryption of Nonpublic Information), and 500.16 (Incident Response Plan) of the Cybersecurity Regulations.

Importantly, Covered Entities under exemption Category 4 continue to be subject to compliance obligations under sections 500.09 (Risk Assessment), 500.11 (Third Party Service Provider Security Policy), 500.13 (Limitations on Data Retention), and 500.17 (Notices to Superintendent) of the Cybersecurity Regulations. Covered Entities under this category are required to file a Notice of Exemption in the form set forth in Appendix B to the Cybersecurity Regulations within 30 days of the determination that the Covered Entity is exempt.

Exemption Category 5: Special Insurance Organizations and Certain Reinsurers

- **Exemption Type 7:** Persons[6] subject to New York Insurance Law Section 1110 (relating to charitable annuity societies) (Section 500.19(f));
- **Exemption Type 8:** Persons subject to New York Insurance Law section 5904 (relating to risk retention groups not chartered in New York) (23 NYCRR 500.19(f)); and
- **Exemption Type 9:** Any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125 (23 NYCRR 500.19(f)).

Individuals and non-governmental entities described under exemption Category 5 are exempt from the requirements of the Cybersecurity Regulations altogether, provided that they do not otherwise qualify as a Covered Entity for purposes of the Cybersecurity Regulations. Unlike the other exemption categories, such individuals and non-governmental entities are not required to file a Notice of Exemption with the NYDFS Superintendent identifying the specific exemption on which the individual or entity relies.

Potential Penalties

Failure to understand the extensive coverage of the Cybersecurity Regulations, as well as the available exemptions, timing and limits of the exemptions under the final regulations, could subject a Covered Entity to potential penalties. Of note, the Cybersecurity Regulations may be enforced by the NYDFS Superintendent pursuant to existing authority available to the Superintendent under New York law. Such enforcement authority includes the ability to issue a consent order, impose a civil money penalty, or enter into a written agreement with a Covered Entity under New York Banking Law §§ 39, 44 and 44-a and relevant provisions of the New York Insurance Law and New York Financial Services Law.

Accordingly, it is imperative that Covered Entities understand and take the appropriate actions to ensure compliance with the Cybersecurity Regulations by the conclusion of the 180-day transitional period on August 28, 2017.

APPENDIX A

Exemptions and Relevant Compliance Obligations under the NYDFS Cybersecurity Regulations Effective March 1, 2017
(Subject to Transitional Periods)

Substantive Requirement	Exemption Category 1*	Exemption Category 2**	Exemption Category 3‡	Exemption Category 4‡‡	Exemption Category 5₸
Section 500.02 Cybersecurity Program.	applicable	exempt	exempt	exempt	exempt
Section 500.03 Cybersecurity Policy.	applicable	exempt	exempt	exempt	exempt
Section 500.04 Chief Information Security Officer.	exempt	exempt	exempt	exempt	exempt
Section 500.05 Penetration Testing and Vulnerability Assessments.	exempt	exempt	exempt	exempt	exempt
Section 500.06 Audit Trail.	exempt	exempt	exempt	exempt	exempt
Section 500.07 Access Privileges.	applicable	exempt	exempt	exempt	exempt
Section 500.08 Application Security.	exempt	exempt	exempt	exempt	exempt
Section 500.09 Risk Assessment.	applicable	exempt	applicable	applicable	exempt
Section 500.10 Cybersecurity Personnel and Intelligence.	exempt	exempt	exempt	exempt	exempt
Section 500.11 Third Party Service Provider Security Policy.	applicable	exempt	applicable	applicable	exempt
Section 500.12 Multi-Factor Authentication.	exempt	exempt	exempt	exempt	exempt
Section 500.13 Limitations on Data Retention.	applicable	exempt	applicable	applicable	exempt
Section 500.14 Training and Monitoring.	exempt	exempt	exempt	exempt	exempt
Section 500.15 Encryption of Nonpublic Information.	exempt	exempt	exempt	exempt	exempt
Section 500.16 Incident Response Plan.	exempt	exempt	exempt	exempt	exempt
Section 500.17 Notices to Superintendent.	applicable	exempt	applicable	applicable	exempt
Section 500.19 Notice of Exemption within 30 Days of Determination.	applicable	applicable	applicable	applicable	exempt

* **Exemption Category 1**: Small Covered Entities - (i) Covered Entities with fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity (Section 500.19(a)(1)); (ii) Covered Entities with less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates (Section 500.19(a)(2)); and (iii) Covered Entities with less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates (Section 500.19(a)(3)).

** **Exemption Category 2**: Employees, Agents, Representatives and Designees - Employees, agents, representatives or designees of a Covered Entity who are covered by the cybersecurity program of the Covered Entity (Section 500.19(b)).

‡ **Exemption Category 3**: Covered Entities without Access to Information Systems or Nonpublic Information - Covered Entities that do not directly or indirectly operate, maintain, utilize or control any Information Systems, and that do not, and are not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information (Section 500.19(c)).

‡‡ **Exemption Category 4**: Insurance Covered Entities without Access to Nonaffiliate Nonpublic Information - Covered Entities under Article 70 of the Insurance Law that do not and are 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) (Section 500.19(d)).

₸ **Exemption Category 5**: Special Insurance Organizations and Certain Reinsurers - Persons subject to New York Insurance Law Section 1110; Persons subject to New York Insurance Law Section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125 (Section 500.19(f)).

AMERICAS

New York

Ian Cuillerier
Partner
T +1 212 819 8713
E icuillerier@whitecase.com

John Donovan
Partner
T +1 212 819 8530
E jdonovan@whitecase.com

David Johansen
Partner
T +1 212 819 8509
E djohansen@whitecase.com

Ernie Patrikis
Partner
T +1 212 819 8200
E ernest.patrikis@whitecase.com

Duane Wall
Partner Of Counsel
T +1 212 819 8453
E dwall@whitecase.com

Francis Zou
Partner
T +1 212 819 8733
E fzou@whitecase.com

Glen Cuccinello
Counsel
T +1 212 819 8239
E gcuccinello@whitecase.com

Washington, DC

Kevin Petrasic
Partner
T +1 202 626 3671
E kevin.petrasic@whitecase.com

Benjamin Saul
Partner
T +1 202 626 3665
E benjamin.saul@whitecase.com

Helen Lee
Counsel
T +1 202 626 6531
E helen.lee@whitecase.com

EMEA

Frankfurt

Benedikt Gillessen
Partner
T +49 69 29994 0
E bgillessen@whitecase.com

Dennis Heuer
Partner
T +49 69 29994 0
E dheuer@whitecase.com

Matthias Kasch
Partner
T +49 69 29994 0
E mkasch@whitecase.com

Andreas Wieland
Partner
T +49 69 29994 1164
E andreas.wieland@whitecase.com

Hamburg

Kai-Michael Hingst
Partner
T +49 40 35005 364
E kmhingst@whitecase.com

London

Francis Fitzherbert-Brockholes
Partner
T +44 20 7532 1400
E ffitzherbert-brockholes@whitecase.com

Stuart Willey
Partner
T +44 20 7532 1508
E swilley@whitecase.com

Carmen Reynolds
Counsel
T +44 20 7532 1421
E creynolds@whitecase.com

ASIA

Tokyo

Seiji Matsuzoe
Partner
T +81 3 6384 3209
E smatsuzoe@whitecase.com

Arthur Mitchell
Senior Counselor
T +81 3 6384 3288
E amitchell@whitecase.com

Hong Kong

Baldwin Cheng
Partner
T +852 2822 0405
E bcheng@whitecase.com

Sharon Hartline
Partner
T +852 2822 8733
E shartline@whitecase.com

Singapore

David Barwise
Partner
T +65 6347 1345
E dbarwise@whitecase.com

[1] Steven R. Chabinsky, Ernest T. Patrikis, and Jeremy Apple, NYS Department of Financial Services Cybersecurity "Regulation Goes Live: Now What?" (March 1, 2017), available at https://www.whitecase.com/publications/article/nys-department-financial-services-cybersecurity-regulation-goes-live-now-what.

[2] NYDFS Press Release, Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyber-Attacks to Take Effect March 1 (Feb. 16, 2017), *available at* http://www.dfs.ny.gov/about/press/pr1702161.htm.

[3] *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise. 23 NYCRR 500.01(a).

[4] *Information System* means a discrete 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. 23 NYCRR 500.01(e).

[5] *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual which 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: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual. 23 NYCRR 500.01(g).

[6] *Person* means any individual or any non-governmental entity, including but not limited to any non- governmental partnership, corporation, branch, agency or association. 23 NYCRR 500.01(i).