REPORT

FINTECH LAW

E-Banking, Payments & Commerce in the Mobile World

March/April 2018 ▪ Volume 21 ▪ Issue 2

NYDFS CYBERSECURITY REGULATIONS: ONE YEAR LATER

By Michael Mancusi, Anthony Raglani, and Kevin Toomey

Michael A. Mancusi is a Partner and Anthony Raglani and Kevin Toomey are Associates in the Financial Services Practice Group of Arnold & Porter in Washington, DC. www.arnoldporter.com/en/services/capabilities/practices/financial-services

Background

In September 2016, New York Governor Andrew Cuomo and Superintendent of the New York State Department of Financial Services (the "DFS") Maria Vullo announced the proposal of cybersecurity regulations described as "groundbreaking" due to their specific applicability to banks, insurance companies, brokers and agents, and other financial services firms and professionals. The regulations were finalized in March 2017 and codified under Part 500 of the DFS's regulations ("Part 500").[1] Roughly one year later, financial institutions subject to Part 500 continue to navigate a number of compliance considerations as the regulations continue to be implemented.

At the time of adoption of Part 500, Governor Cuomo indicated that the regulations are intended to serve as a meaningful tool in combatting cybercrime and in preventing and mitigating the effects of information security breach incidents.[2] The DFS has since made clear that supervision and enforcement of compliance with Part 500 will be a priority. Specifically, Superintendent Vullo announced that cybersecurity compliance will be incorporated into the examinations of all DFS-supervised entities and questions related to cybersecurity will be added to the DFS's "first-day letters" at the commencement of examinations.[3] Moreover, the DFS and other New York law enforcement officials, such as New York County District Attorney Cyrus R. Vance, Jr., have indicated that all necessary actions will be taken to prevent cybercrime, including by using Part 500 as a proactive tool to protect consumers and the financial services industry.[4]

Although Part 500 contains provisions that are similar to those imposed upon banks and securities firms under regulations and guidance issued by federal banking and securities agencies, Part 500 differs in certain details and imposes substantial reporting obligations upon covered institutions and persons. Moreover, Part 500 presents complex questions of applicability for many entities, including entities with minimal contacts with New York State or those which are reliant upon the information systems of otherwise exempt entities. The first examinations of compliance with the regulations are approaching and the DFS will almost cer-

tainly adopt a thorough and aggressive approach to supervision and enforcement of Part 500. Accordingly, financial institutions must take care to understand the full scope of their regulatory obligations, certain aspects of which are being evaluated and refined by the DFS on an ongoing basis as the implementation period unfolds, further complicating the already difficult task of compliance.

Overview of Part 500

Scope. A "Covered Entity" is defined under Part 500 as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."[5] DFS guidance establishes that New York branch offices of out-of-state domestic banks are not "Covered Entities"; however, New York branch offices, agencies and representative offices of foreign banking organizations are subject to compliance with Part 500.[6] Brokers, dealers and investment advisers—which are not required to register under the New York Banking, Insurance or Financial Services Laws and are not supervised by the DFS—are not subject to Part 500 absent engagement in a DFS-regulated activity either directly or indirectly through affiliates or subsidiaries.

With respect to the New York branches of out-of-state domestic banks, DFS guidance provides specifically that the DFS will defer to the home state supervisors of such banks for supervision and examination of the bank's New York branches, with the caveat that DFS may elect to coordinate with the home state in such supervision and examination. In addition, the DFS notes that the New York branch offices of out-of-state domestic banks are, in general, required to comply with New York law and may be examined by the DFS notwithstanding its established approach to oversight of such branches. Accordingly, the DFS strongly encourages all financial institutions, including New York branch offices of out-of-state domestic banks, to adopt cybersecurity protections consistent with the safeguards and protections of Part 500.[7]

Part 500 provides limited exemptions from compliance for certain entities and individuals.[8] Specifically, the following entities and individuals may claim an exemption from Part 500, either in full or in part depending upon the applicable exemption:

- Covered Entities with fewer than 10 New York employees and independent contractors (including those of affiliates), less than $5 million in gross annual revenue from New York business operations in each of the last three fiscal years (including such revenue of affiliates), or less than $10 million in year-end total assets (including the total assets of affiliates).

- Covered Entities that do not directly or indirectly operate, maintain, utilize or control any "Information Systems"[9]and that do not, and are not required to, directly or indirectly, control, own, access, generate, receive or possess "Nonpublic Information" ("NPI").[10]

- Employees, agents, representatives and designees of a Covered Entity who are themselves Covered Entities (*e.g.*, individually licensed insurance producers employed by or under contract with a licensed insurance producer business entity), provided

that such individuals or entities are covered entirely by the cybersecurity program of another Covered Entity.

- Certain captive insurance companies registered under Article 70 of the New York Insurance Law that do not, directly or indirectly, control, own, access, generate, receive or possess NPI other than certain information relating to its corporate parent company or affiliates thereof.

As discussed further below, any entity or individual that qualifies for one of the above exemptions must file a notice of exemption with the DFS within 30 days of the determination of qualification.[11] Importantly, with the exception of the exemption provided for employees, agents, representatives and designees of Covered Entities, and depending upon the specific exemption claimed, these provisions may not not exempt Covered Entities from the core elements of Part 500, including the requirement to development a compliant cybersecurity program and corresponding policies and procedures.[12] Moreover, Covered Entities that qualify for one of the above-described exemptions are nonetheless required to file an annual certification of compliance with the provisions of Part 500 applicable to the Covered Entity.[13]

Cybersecurity Program Requirements. Part 500 requires, among other things, that Covered Entities:[14]

- Maintain a cybersecurity program and corresponding policies and procedures reasonably designed to protect the confidentiality, integrity and availability of Information Systems;
- Designate a qualified individual responsible for overseeing and implementing the cybersecurity program (a "Chief Information Security Officer" or "CISO"), who is also required develop a written report for management, at least annually, that addresses key cybersecurity issues affecting the Covered Entity;
- Include risk-based continuous monitoring or periodic penetration testing or vulnerability assessments in their cybersecurity programs;[15]
- Maintain secure systems capable of reconstructing material financial transactions which include audit trails designed to detect and respond to "Cybersecurity Events" that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.[16]
- Limit user access privileges to Information Systems that provide access to NPI and to review such access controls periodically;
- Conduct a periodic risk assessment of Information Systems, updated as reasonably necessary to address changes to such Systems, business operations or information collection activities;[17]
- Develop policies and procedures designed to ensure the security of Information Systems and NPI accessible to, or held by, third-party vendors;
- Implement risk-based policies to monitor the activity of internal users, detect unauthorized access or use of NPI and provide regular cybersecurity awareness training for all personnel;

- Implement risk-based controls, including encryption, to protect NPI held or transmitted by the Covered Entity both in transit over external networks and at rest; and
- Establish a written security incident response plan for use in responding to and recovering from any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of the Covered Entity's business operations.

Filing and Recordkeeping Obligations. Part 500 requires each Covered Entity to submit to the DFS annually, by February 15, a written certification of compliance with the applicable requirements of Part 500 for the prior calendar year. Covered Entities need not submit any supporting documentation with their certification filing; however, records, schedules and data supporting the certificate must be maintained for examination by the DFS for a period of five years. Documentation of any areas of compliance that require material improvement, updating or redesign, and any planned remedial efforts will be of particular importance.[18] The requirement to certify compliance has been interpreted broadly by the DFS. For example, as noted above, Covered Entities that qualify for a limited exemption from Part 500 are generally required to file certifications, even if not subject to the majority of Part 500 or if covered by the cybersecurity program of another Covered Entity that has itself certified compliance. In addition, although a Covered Entity may rely upon the cybersecurity program of an affiliate for purposes of compliance with Part 500, the certification requirement may not be met by the affiliate, meaning that separate certifications will need to be filed by each affiliated entity.[19]

The completion of a certification of compliance may be costly for several Covered Entities and will require directors and senior managers to obtain actual and, in some instances, extensive knowledge of information systems and related compliance controls. Covered Entities' first certifications were required to be filed on February 15, 2018. According to the DFS, a substantial number of DFS licensees failed to submit their required certifications or did not do in accordance with DFS filing guidance.[20] This development reflects certain complexities and uncertainty regarding the scope of Part 500 and the DFS's expectations for compliance.

Part 500 also requires Covered Entities that qualify for a limited exemption to file an initial notice of exemption with the DFS and to update such notices as may be required. This filing requirement extends even to employees, agents, representative and designees of a Covered Entity who are covered by the cybersecurity program of their employer and are fully exempt from Part 500. Under such circumstances, the DFS will allow certain Covered Entities to file a single notice of exemption on behalf of multiple exempt filers, but only if the Covered Entity (i) employs 50 or more individuals who are themselves Covered Entities and are reliant upon the same exemption and (ii) seeks and receives the permission of the DFS to do so.[21]

Finally, Covered Entities must notify the DFS within 72 hours of the determination of an occurrence of a Cybersecurity Event impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory

agency or any other supervisory body, or that has a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity. This requirement adds to existing notification requirements that apply generally to most Covered Entities under state information security breach notification statutes and, with respect to banking organizations, federal interagency information security standards.[22] Moreover, the notification requirement may apply not only to successful cyberattacks and actual information security breach incidents, but also to certain *unsuccessful* cyberattacks. DFS guidance indicates that it expects Covered Entities to provide notice of unsuccessful cyberattacks that appear "particularly significant" and "sufficient to raise a serious concern" based on the Covered Entity's risk assessment.[23] The DFS has clarified that any Cybersecurity Event that involves material consumer harm must be reported.[24]

Implementation Period. Part 500 became effective on March 1, 2017, but several of its provisions are subject to longer compliance transition periods as set forth below.

Section	Statutory Heading	Compliance Date
500.02	Cybersecurity Program	August 28, 2017
500.03	Cybersecurity Policy	August 28, 2017
500.04(a)	Designation of CISO	August 28, 2017
500.04(b)	Annual Report of CISO	March 1, 2018
500.05	Penetration Testing and Vulnerability Assessments	March 1, 2018
500.06	Audit Trail	September 3, 2018
500.07	Access Privileges	August 28, 2017
500.08	Application Security	September 3, 2018
500.09	Risk Assessment	March 1, 2018
500.10	Cybersecurity Personnel and Intelligence	August 28, 2017
500.11	Third Party Service Provider Security Policy	March 1, 2018
500.12	Multi-Factor Authentication	March 1, 2018
500.13	Limitations on Data Retention	September 3, 2018
500.14(a)	Risk-Based Policies for Monitoring the Use of NPI	September 3, 2018
500.14(b)	Cybersecurity Awareness Training	March 1, 2018
500.15	Encryption of NPI	September 3, 2018
500.16	Incident Response Plan	August 28, 2017
500.17(a)	Notice to DFS of Cybersecurity Event	August 28, 2017
500.17(b)	Notice to DFS (Annual Certifications)	February 15, 2018

Considerations for Covered Entities

Part 500 has already increased the compliance burden of Covered Entities and such costs are likely to continue to rise as the DFS begins to examine Covered Entities for compliance, which

the DFS has indicated will occur as part of a Covered Entity's next scheduled full scope examination. The DFS will likely examine for compliance with, and include information and document requests relating to, the provisions of Part 500 in effect on the as-of date of the examination. Accordingly, Covered Entities should expect a more comprehensive review of their operations in examinations as of September 3, 2018 or later, at which point the vast majority of Part 500 will be effective. Notable ongoing considerations for Covered Entities include the following, among others.

Liability Related to Annual Certification of Compliance. A significant driver of liability relates to Part 500's certification requirement. Superintendent Vullo has commented that the certification is a "critical pillar for the cybersecurity programs of all DFS-regulated entities."[25] The DFS may, however, take a flexible approach to enforcement of the certification requirement during the initial period of compliance. For example, as of the initial filing deadline many provisions of Part 500 were not yet effective, including the cybersecurity risk assessment required under Section 500.09, which is intended to inform the design of a Covered Entity's cybersecurity program. Accordingly, notwithstanding any certifications that have already been filed, the DFS has acknowledged that it expects Covered Entities to revise and update their cybersecurity programs based on risk assessment findings and to incorporate additional controls for provisions of Part 500 that are subject to longer compliance transitional periods.[26]

Beyond the initial period of compliance, the certification requirement provides the DFS with a tool to initiate enforcement actions against any Covered Entity based on deficiencies in the Covered Entity's cybersecurity program that are inconsistent with any prior certifications. Moreover, the DFS may seek to hold Covered Entity's CISOs or certifying directors or managers personally liable for any compliance deficiencies. Although Covered Entities' cybersecurity programs are intended to be risk-based and updated periodically to account for technological developments and changes in business operations, it is unclear to what extent the DFS will accept a Covered Entity's certification when significant improvements or updates to the Covered Entity's cybersecurity program are required and not yet implemented. In any event, it is critical for Covered Entities to develop a comprehensive internal record supporting any certification of compliance that includes documentation of the processes used to identify any cybersecurity vulnerabilities or compliance shortcomings and any remedial measures taken as a result.

Perhaps the first meaningful indicator of the DFS's approach to enforcement of Part 500 will be its response to Covered Entities that either filed their initial certifications of compliance well after the February 15, 2018 deadline or neglected to file entirely. Indeed, in early March the DFS notified a number of Covered Entities of their failure to file a timely certification. In related guidance published shortly thereafter, the DFS did not indicate expressly that such Covered Entities would be penalized for a late filing, but stated that certifications should be filed "as soon as possible" and that any failure to file will be treated as an indication of a substantive deficiency in a Covered Entity's cybersecurity program.[27] The DFS's guidance leaves open the possibility of the imposition of monetary penalties and other fines for a substantially-late filing or for the failure to

file and the extent of any such penalties may serve as a preview of the DFS's long-term approach to examination and enforcement of Part 500.

Information Systems Issues. Covered Entities are faced with challenging strategic issues regarding existing information systems. For example, Part 500's requirements for multi-factor authentication, risk-based authentication and the encryption of NPI may be difficult to implement on legacy information systems and across networks utilized by Covered Entities. The implementation of wholesale information systems changes may be costly and time consuming, while the design and implementation of compensating controls within existing systems may require a highly-skilled CISO and information security staff and the reliance upon such alternative controls could further expose a Covered Entity to scrutiny in connection with its certification of compliance.[28]

In addition, because financial institutions and their subsidiaries and affiliates often use interconnected information systems, certain exempt institutions may be required to develop enterprise-wide controls that are compliant Part 500 due to the existence of subsidiaries or affiliates that are Covered Entities. For example, although domestic out-of-state banks and their New York branch offices are not treated as Covered Entities and, as applied to national banks, Part 500 is likely preempted by federal law, to the extent such banks maintain DFS-licensed and supervised subsidiaries or affiliates that rely upon the banks' enterprise-wide information systems, such systems may be required to conform to Part 500 in order to allow Covered Entity subsidiaries and affiliates to certify compliance.

Cybersecurity Event Reporting. Covered Entities have a 72-hour window within which to identify, investigate and, if necessary, report to the DFS the occurrence of a Cybersecurity Event. This time frame is, in general, much shorter and less flexible than those established under applicable information security breach notification laws, regulations and guidance. Covered Entities must therefore ensure that their information systems monitoring and vulnerability testing procedures are functional and effective and their information security breach incident response plans are comprehensive, known to all personnel, mapped to applicable reporting requirements and reviewed and updated periodically. As with other aspects of Part 500, the extent to which the DFS will strictly enforce any late reporting of Cybersecurity Events remains to be seen, but Covered Entities that submit substantially-late notices to the DFS may be subject to scrutiny given that a central focus of Part 500 is the prevention of cyberattacks and the mitigation of consumer harm related to information security breach incidents.

Long-Term Strategic Issues. Depending upon the DFS's long-term actions with respect to supervision and enforcement of Part 500, Covered Entities may wish to consider various strategic alternatives for managing institutional and personal regulatory risk, including charter conversion (to a new home state or a national bank charter), relocation, business model changes and reorganization of New York subsidiaries and affiliates subject to Part 500.

ENDNOTES:

[1]N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01 *et seq*.

[2]Press Release, New York Department of

Financial Services, Governor Cuomo Announces First-in-the-Nation Cybersecurity Regulation Protecting Consumers and Financial Institutions from Cyberattacks to Take Effect March 1 (Feb. 16, 2017) ("New York is the financial capital of the world, and it is critical that we do everything in our power to protect consumers and our financial system from the ever increasing threat of cyber-attacks. . . . These strong, first-in-the-nation protections will help ensure this industry has the necessary safeguards in place in order to protect themselves and the New Yorkers they serve from the serious economic harm caused by these devastating cybercrimes.") (hereinafter "Adopting Press Release").

[3]Press Release, New York Department of Financial Services, DFS Superintendent Vullo Issues Cybersecurity Filing Deadline Reminder (Jan. 22, 2018).

[4]*Id.* ("As the DFS continues to implement its landmark cybersecurity regulation, we will take proactive steps to protect our financial services industry from cyber criminals."); Adopting Press Release ("[D]efeating cybercrime requires not only prosecuting it, but taking all necessary actions to prevent it. DFS's cybersecurity regulation will be a crucial tool in the ongoing battle against cybercrime and identity theft . . . .").

[5]N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(c).

[6]DFS, Frequently Asked Questions Regarding 23 N.Y.C.R.R. Part 500, Questions 16 & 24 (last updated Mar. 23, 2018) (hereinafter the "DFS FAQ"). The DFS's position with respect to the branch offices of out-of-state domestic banks applies to any office that meets the definition of "branch" under Section 222 of the New York Banking Law—*i.e.*—"any office of a banking institution at which deposits are received, checks paid or money lent," including the "principal or main office of a banking institution," but generally excluding "automated teller machines or other electronic facilities."

[7]DFS FAQ, Question 16.

[8]N.Y. COMP. CODES R. & REGS. tit. 23, § 501.19(a)-(d).

[9]The term "Information Systems" is defined as "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." *Id. §* 500.01(e).

[10]The term "Nonpublic Information" is defined as:

> All electronic information that is not Publicly Available Information [as that term is defined under Part 500] 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.

Id. § 500.01(g).

[11]Certain exempt entities are not required to submit a notice of exemption, such as certain charitable annuity societies, insurance risk retention groups and accredited or certified reinsurers. *See id. §* 500.19(f).

[12]For example, any Covered Entity that qualifies as an exempt smaller entity under Section 500.19(a) is required to comply with Sections 500.02 (Cybersecurity Program), 500.03 (Cyber-

security 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 the DFS).

[13]*See* New York Department of Financial Services, Key Questions About the Recent Cyber Regulation Notice (Mar. 5, 2018).

[14]*See generally* Vol. 34 N.Y. Reg. Issue 9 at 3 (Mar. 1, 2017).

[15]DFS guidance provides that there is no specific technology that is required to be used in order to have an effective continuous monitoring program; however, according to the DFS, 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. *See* DFS FAQ, Question 28.

[16]A "Cybersecurity Event" is defined as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System." N.Y. COMP. CODES R. & REGS. tit. 23, § 500.01(d).

[17]Covered Entities' risk assessments are required to be documented and carried out in accordance with applicable policies and procedures which themselves must include criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity, criteria for assessing the confidentiality, integrity, security and availability of Information Systems and NPI, and requirements describing how identified risks will be mitigated or accepted, and how the Covered Entity's cybersecurity program will address such risks. *See id.* § 500.09.

[18]*See* DFS FAQ, Question 10.

[19]*See id.*, Question 21.

[20]*See* New York Department of Financial Services, Key Questions About the Recent Cyber Regulation Notice (Mar. 5, 2018).

[21]DFS FAQ, Question 14.

[22]*See*, *e.g.*, N.Y. GEN. BUS. LAW § 899-aa (New York State's information security breach notification statute, which applies generally to any person or business that owns or licenses computerized data which includes the "private information" of consumers); *see also* 12 C.F.R. Part 225. Appx. F; *Id.* Part 364, Appx. B; *Id.* Part 30, Appx. B.

[23]DFS FAQ, Question 15.

[24]*Id.*, Question 19.

[25]Press Release, New York Department of Financial Services, DFS Superintendent Vullo Issues Cybersecurity Filing Deadline Reminder (Jan. 22, 2018).

[26]DFS FAQ, Question 25.

[27]New York Department of Financial Services, Key Questions About the Recent Cyber Regulation Notice (Mar. 5, 2018).

[28]Section 500.15 of Part 500, which requires encryption of NPI, permits a Covered Entity to use alternative compensating controls if its CISO determines that encryption is not feasible. To the extent this option is exercised, the Covered Entity's CISO must review the effectiveness of the compensating controls on an annual basis. Covered Entities should therefore be prepared to present the DFS with a comprehensive record of any decision to use alternative compensating controls in lieu of encryption in connection with their certifications of compliance.