




Department of
Financial Services

MEMORANDUM

TO: Chief Executive Officers of DFS Regulated Institutions

FROM: Superintendent Maria T. Vullo 

DATE: December 21, 2018

RE: DFS Cybersecurity Regulation -- First Two Years and Next Steps

This memorandum provides an update on the New York Department of Financial Services (DFS)'s cybersecurity regulation, 23 NYCRR 500, which became effective March 1, 2017, with a two-year implementation period. Please share this memorandum with relevant personnel responsible for your institution's cybersecurity compliance.

The regulation requires all DFS regulated entities, subject to certain exemptions, to adopt the core requirements of a cybersecurity program, including a cybersecurity policy, effective access privileges, cybersecurity risk assessments, and training and monitoring for all authorized users, among other requirements. The regulation also requires the establishment of governance processes to ensure senior attention to these important protections. The final effective date for the regulation will be March 1, 2019, by which time, under section 500.11, DFS regulated entities are required to have written policies and procedures that are based on a risk assessment to ensure the security of nonpublic information and information systems that are accessed or held by third party service providers.

Accordingly, by March 1, 2019, all banks, insurance companies, and other financial services institutions and licensees regulated by DFS will be required to have a robust cybersecurity program in place that is designed to protect consumers' private data; a written policy or policies that are approved by the Board of Directors or a Senior Officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial services industry including encryption and multifactor authentication. The regulation sets forth certain limited exemptions, many of which still require certain cybersecurity programs and practices.

As Superintendent, I have made clear that the purpose of the DFS cybersecurity regulation is to bolster the financial services industry's defenses against cybersecurity attacks, in order to protect our markets and consumers' private information. The governance framework set forth in the regulation, along with DFS's ongoing oversight, including in regular and target examinations, are intended to assist in the bolstering of the industry's cybersecurity defenses, for the protection of industry, overall markets and consumers. Consistently with these important objectives, DFS examiners have been including cybersecurity in all regular examinations across the Department. Furthermore, DFS has established internal policies and procedures for the review and response to confidential information provided by regulated entities to DFS as part of the regulation's notice and other procedures.

Notices of Breach

Importantly, the DFS cybersecurity regulation requires regulated entities and licensed persons to submit notices to the Department of cybersecurity events as defined in the regulation to include both successful and certain unsuccessful attempts. The purpose of this notice provision is to provide the Department with information relevant to its supervision of the financial services industry, including to provide confidential assistance to regulated entities with respect to information learned by the Department that could be useful to further bolster industry's cybersecurity protections. The confidentiality of the Department's specific interactions with regulated entities with respect to cybersecurity is protected by law, including the Banking Law, Insurance Law and Financial Services Law. While individual interactions are confidential, this memorandum provides a broad overview of the Department's practices and general themes with respect to the Department's information gathering over the past year.

Pursuant to the regulation, the Department has received approximately 1,000 notices of cybersecurity events from regulated institutions. DFS investigators review these notices and, in consultation with our examination and supervisory teams, assess the information and take appropriate actions to address any concerns that relate to institutions' cybersecurity protections. In some cases, based on the information provided and any responses already undertaken by the regulated entity, no further action by DFS is deemed warranted. In other cases, DFS professionals may identify from the information provided a circumstance or trend that subject to confidentiality warrants providing certain information to other regulated entities regarding a potential threat. For example, the identification of a cyber breach relating to a third-party vendor that contracts with multiple institutions in a certain sector may warrant DFS providing information to those other DFS regulated institutions. In appropriate circumstances, DFS professionals may take other steps, including making sure that the appropriate law enforcement bodies have been alerted, that the institution is addressing any impacted consumer, and of critical importance that necessary steps are being taken to close and remedy the system issue that led to the breach. All of these actions are taken by DFS in consultation with the regulated institution in question, with the goal of protecting the institution and other DFS regulated institutions, as well as the customers of the affected institutions.

In general, DFS's experience based on reports of cybersecurity events has only emphasized the importance of Part 500's requirements, including the need for strong access controls and the protection of email systems including authorized users and training of employees. Part 500.03 requires all companies, including most small companies that are entitled to a limited exemption, to have policies and procedures for access controls. Importantly, the majority of successful breaches involve common software technology used throughout business operations and have involved phishing attacks, social engineering threats, and issues relating to password composition and security and email security.

More specifically, a significant number of the events reported to DFS involved breaches that stemmed from employees providing credentials in response to attractive emails that trick a user to provide confidential information. In these cases, the intruder sends a legitimate-seeming e-mail to a company's employee or employees. These attacks are carefully planned to appear from a source that the employee will trust, perhaps even appear to be an email from a customer or client of that employee and a subject that will peak their interest. The employee is prompted

to enter his or her e-mail credentials, and the intruder gains access to the company's e-mails on the system, which can contain consumers' personal identifying information.

These many events remind us to make sure that all persons who can access a company's systems have the proper protections, and are using the appropriate protections. Third parties who access a company's systems or data can cause serious breaches where such third parties were using unsecured email accounts. Other access issues that arise include "credentials churning" attacks, by which the company's access portal is bombarded with access attempts using usernames and passwords from other breaches. In these situations, the attackers know that many users reuse the same username and password for numerous websites, and therefore try to use the user names and passwords that have been the subject of known breaches to see if they will allow access here.

In many cases, the protections required by the DFS regulation could have prevented these incidents: for example, strong access controls and training as required by the regulation are critical to avoiding the phishing attacks that threaten the market. We also emphasize the need for education and training which can help ensure that all parts of the organization are aware of and follow proper cybersecurity procedures. DFS has emphasized working with its licensees and regulated persons to improve their programs, and licensees should embrace opportunities to improve and advance their cybersecurity readiness and systems. While all aspects of the DFS regulation are important, recent attacks on emails and transmissions highlight the importance of full compliance with the following provisions of the DFS regulation:

- Multi-factor Authentication (500.12): Breaches occur more easily when the company does not have multi-factor authentication in place, or where the multi-factor authentication protection malfunctioned. In fact, as more businesses have adopted multi-factor authentication, the Department has seen a decline of reportable events.
- Encryption (500.15): Strong access control and encryption for data in transit and at rest mitigate the loss and are critically important.
- Training (500.14): Ongoing training is essential. All staff needs basic cybersecurity training to avoid events like successful phishing scams, and ongoing reminders and training to ensure protections from errors that could have significant consequences.

Certificate of Compliance

DFS's regulation requires each entity to conduct an annual review and assessment of its cybersecurity program's achievements, deficiencies and overall compliance with regulatory standards and to certify the institution's compliance with the regulation on an annual basis. The DFS compliance certification is a critical governance pillar for the cybersecurity program of all DFS regulated entities. The first certification deadline was February 15, 2018, which was successful and provided DFS with information from which we have been working to improve our processes. DFS currently is preparing for the second annual certifications of compliance due by **February 15, 2019**. By this date, all regulated entities and licensed persons must file a Certification of Compliance covering calendar year 2018, confirming the entity or person's compliance with the DFS cybersecurity regulation. In January 2019, prior to the February 15, 2019 certification deadline, any regulated person or licensed entity that is entitled to an

exemption must file a new Notice of Exemption notifying DFS of the current exempt status. All of these filings must all be filed electronically via the improved DFS cybersecurity portal.

2019 Filing Calendar: Notices of Exemption and Certificates of Compliance

Any DFS regulated entity or licensed person that is entitled to an exemption must file a Notice of Exempt status for the calendar year 2019 prior to filing the annual certification for calendar year 2018 on February 15, 2019. This requirement applies even if you previously notified DFS of your exemption status, as the assessment of exemption status is an annual requirement.

Prior to February 15, 2019, all regulated institutions must file the annual certification of compliance, covering calendar year 2018, setting forth the institution's compliance with the cybersecurity regulation for those provisions that were applicable in 2018. The DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

Additional information concerning the DFS cybersecurity regulation is available on the DFS Website including:

- 2019 Cybersecurity Filing Schedule
- Information concerning requirements under the cybersecurity regulation
- Step by step instructions regarding filing exemptions and compliance certifications
- FAQs and other helpful information concerning the DFS cybersecurity regulation
- Information concerning DFS Cybersecurity Secure Portal for filings

Conclusion

During the prior year, DFS and its regulated entities and licensed persons collectively have enhanced the financial services industry's cybersecurity protections for New York, providing national standards and leadership on this critically important issue. Through our ongoing supervision and examinations, DFS has noted many institutions' increased adoption of governance and system protections to protect consumers and industry data. The cybersecurity events that have been filed with DFS and any deficiencies identified through the certification and examination processes indicate both the severity of this ongoing threat, as well as the dedicated work being undertaken to combat these threats, bolster defenses, and prevent future attacks. As the DFS cybersecurity regulation reaches its final implementation deadline on March 1, 2019, and with DFS examination and supervision systems in place, DFS professionals are ready to continue to work with regulated institutions and other stakeholders to improve cybersecurity protections for New York's financial services industry.

**NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500**

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 Introduction.

The New York State Department of Financial Services (“DFS”) has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization’s cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity’s cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *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.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) *Covered Entity* means 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.

(d) *Cybersecurity Event* means 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.

(e) *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.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

- (1) Knowledge factors, such as a password; or
- (2) Possession factors, such as a token or text message on a mobile phone; or
- (3) Inherence factors, such as a biometric characteristic.

(g) *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.

(h) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

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

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

Section 500.02 Cybersecurity Program.

(a) *Cybersecurity Program*. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Section 500.03 Cybersecurity Policy.

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

- (j) physical security and environmental controls;
- (k) customer data privacy;
- (l) vendor and Third Party Service Provider management;
- (m) risk assessment; and
- (n) incident response.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and

(3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

(1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;

(2) the Covered Entity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the Covered Entity;

(4) overall effectiveness of the Covered Entity's cybersecurity program; and

(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail.

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) 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.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 500.09 Risk Assessment.

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible

to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Section 500.14 Training and Monitoring.

As part of its cybersecurity program, each Covered Entity shall:

(a) implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

- (2) the goals of the incident response plan;
- (3) the definition of clear roles, responsibilities and levels of decision-making authority;
- (4) external and internal communications and information sharing;
- (5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;
- (6) documentation and reporting regarding Cybersecurity Events and related incident response activities;
and
- (7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

- (1) Cybersecurity Events 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
- (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

Section 500.18 Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

- (a) Limited Exemption. Each Covered Entity with:

(1) 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, or

(2) 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, or

(3) less than \$10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,

shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part 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.

(c) A Covered Entity 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 shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that 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) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 500.20 Enforcement.

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

Section 500.21 Effective Date.

This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

Section 500.22 Transitional Periods.

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

Section 500.23 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

(Covered Entity Name)

February 15, 20____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of _____ (date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended __ (year for which Board Resolution or Compliance Finding is provided) complies with Part ____.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name) _____

Date: _____

[DFS Portal Filing Instructions]

(Covered Entity Name)

(Date)_____

Notice of Exemption

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- Section 500.19(a)(1)
- Section 500.19(a)(2)
- Section 500.19(a)(3)
- Section 500.19(b)
- Section 500.19(c)
- Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_____

Date: _____

(Title)

(Covered Entity Name)

[DFS Portal Filing Instructions]



Industry Guidance

Information about 2019 DFS Cybersecurity Filing Requirements

January 2019 – Exemption Filing Period

*February 15, 2019 – Certification of Compliance
due*

The DFS Cybersecurity Portal has been redesigned to assist users with their filings. To ensure that filings are matched to the appropriate Covered Entity or licensed person, we encourage the use of an identifying number when filing. The identifying numbers are: NYS License number, NAIC/NY Entity number, NMLS number or Institution number. Please make sure that you have your license number available when you make your filing. A look-up feature is included in the portal for anyone who does not know which number to use.

Exemptions – Exemptions filed in 2017 and 2018 have expired. Any DFS regulated entity or licensed person that is currently entitled to an exemption must file an Initial [Notice of Exempt](#) status prior to the due date for annual Certificates of Compliance on February 15, 2019.

[More information on exemptions.](#)

Certification of Compliance – All Covered Entities and licensed persons who are not fully exempt from the Regulation are required to submit a Certification of Compliance no later than February 15, 2019 attesting to their compliance for the 2018 calendar year.

[Filing Instructions to assist with the process](#)

Receipts - You will receive an email that includes a receipt number for all filings you complete. The receipt will indicate the year the filing was made. The receipt will also indicate the type of filing made: Notices of Exemption will have a receipt number that begins with the letter “E.” Certifications of

Compliance will have a receipt number that starts with the letter “C.” It is suggested that you maintain a copy of this email in your records for future reference.

Questions about filings should be directed to DFS at cyberregcomments@dfs.ny.gov.



DFS Portal

Who We Supervise

Institutions That We Supervise

The Department of Financial Services supervises many different types of institutions. Supervision by the Department may entail chartering, licensing, registration requirements, examination, and more.

[Learn More](#)

Department of Financial Services

About Us

[Our History](#)

[Mission and Leadership](#)

[Careers With DFS](#)

[Procurement](#)

[Advisory Boards](#)

State Laws & Regulations

[State Codes, Rules &](#)

[Regulations](#)

[State Laws \(LBDC\)](#)

[State Bills & Laws \(Senate\)](#)

Website

[Accessibility](#)

[Disclaimer](#)

[Language Access](#)

[Privacy Policy](#)

[Site Map](#)

Language Assistance

[English](#)

[Español](#)

[Kreyòl ayisyen](#)

[Polski](#)

[Русский](#)

[বাঙালি](#)

[中文](#)

[한국어](#)

Connect With Us



[Facebook](#)



[Instagram](#)



[Twitter](#)

Cybersecurity Regulation Exemptions

23 NYCRR 500.19

Section 19 of the DFS cybersecurity regulation contains several exemptions. Each have been crafted to meet the particular circumstances of the Covered Entity, including smaller organizations, licensed persons who are following the cybersecurity program of another regulated company, or those who do not have any Information Systems and Nonpublic Information. These exemptions have been tailored to address these particular circumstances. Most exemptions are limited in nature and require Covered Entities to still comply with some provisions of the Regulation.

Filing Requirements: All regulated persons and companies that wish to claim an exemption must file with DFS a Notice of Exemption stating their current exempt status prior to the certification deadline of February 15, 2019. Previously filed exemptions are set to expire and must be refiled. No Notice of Exemption filed in 2017 or 2018 need to be removed or terminated. Any DFS regulated entities or licensed person that is entitled to an exemption must file an initial exempt status during January 2019 prior to filing their annual certification. Thereafter, changes in this status should be made through an amendment or termination filing.

To get started please **visit the DFS Cybersecurity Portal:**



Cyber Portal

[Instructions: Filing a New or Initial Notice of Exemption \(PDF\)](#)

Exemption Guidance: To complete a Notice of Exemption, you must identify all exemptions that meet your circumstances. The following are explanations of the exemptions provided for in 23 NYCRR 500.19:

Industry Guidance

exemption when a Covered Entity has fewer than 10

contractors. This is a limited exemption and you must still

design and implement a cybersecurity program that meets some but not all the regulatory requirements. This includes submitting an annual Certification of Compliance.

- 500.19(a)(2) – You are entitled to this exemption when a Covered Entity has less than \$5,000,000 in gross annual revenue in each of the last 3 fiscal years from NY business. This is a limited exemption and you must still design and implement a cybersecurity program that meets some but not all the regulatory requirements. This includes submitting an annual Certification of Compliance.
- 500.19(a)(3) – You are entitled to this exemption when a Covered Entity has less than \$10,000,000 in year-end total assets. This is a limited exemption and you must still design and implement a cybersecurity program that meets some but not all the regulatory requirements. This includes submitting an annual Certification of Compliance.
- 500.19(b) – You are entitled to this exemption when you are an employee, agent, representative or designee of another Covered Entity and you are following that entity’s cybersecurity program. Under this exemption persons do not need to create their own program, but will be required to identify the Covered Entity’s whose program you are following to claim this exemption. This exemption requires an employee, agent, representative or designee to be fully covered by the program of another Covered Entity. To submit a Notice of Exemption under 500.19(b) you will be required to provide the name and address of the covered entity that supports the cybersecurity program you are following and the name of an appropriate representative who can confirm that cybersecurity program.
- 500.19(c) – You are entitled to this exemption if you are a Covered Entity that does not utilize an Information System and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information. This is a limited exemption and you must still complete an annual risk assessment to confirm that the company continues to be entitled to this exemption and meet some but not all the regulatory requirements. This includes submitting an annual Certification of Compliance.
- 500.19(d) – A captive insurance company that does not control nonpublic information other than information relating to its corporate parent company. This is a limited exemption and you must still complete an annual risk assessment to confirm that the company continues to be entitled to this exemption and meet some but not all the regulatory requirements. This includes submitting an annual Certification of Compliance.

Regulations that you still need to comply with if you are eligible for any exemptions:

Exemption	Exempt From	Still Required
500.19 (a) (1) Fewer than 10 employees working in NYS	500.04- Chief Information Security Officer 500.05- Penetration Testing and Vulnerability Assessments 500.06- Audit Trail	500.02- Cybersecurity Program 500.03- Cybersecurity Policy 500.07- Access Privileges 500.09- Risk Assessment 500.11- Third Party Service Provider Security Policy
500.19 (a) (2) Less than \$5 million in gross annual revenue	500.08- Application Security 500.10- Cybersecurity Personnel and Intelligence 500.12- Multi-Factor Authentication	500.13- Limitations on Data Retention 500.17- Notices to Superintendent 500.18- Confidentiality
500.19 (a) (3) Less than \$10 million in year-end total assets	500.14- Training and Monitoring 500.15- Encryption of Nonpublic Information 500.16- Incident Response Plan	500.19- Exemptions 500.20- Enforcement 500.21- Effective Date 500.22- Transitional Periods 500.23- Severability

Exemption	Exempt From	Still Required
500.19 (c) Does not control any information systems and nonpublic information	500.02- Cybersecurity Program 500.03- Cybersecurity Policy 500.04- Chief Information Security Officer	500.09- Risk Assessment 500.11- Third Party Service Provider Security Policy 500.13- Limitations on Data Retention
500.19 (d) Captive insurance companies that do not control nonpublic information other than information relating to its corporate parent company	500.05- Penetration Testing and Vulnerability Assessments 500.06- Audit Trail 500.07- Access Privileges 500.08- Application Security 500.10- Cybersecurity Personnel	500.17- Notices to Superintendent 500.18- Confidentiality 500.19- Exemptions 500.20- Enforcement

Industry Guidance

500.13- Multi-Factor Authentication	500.21- Effective Date
500.14- Training and Monitoring	500.22- Transitional Periods
500.15- Encryption of Nonpublic Information	500.23- Severability
500.16- Incident Response Plan	

Filings of Behalf of Others - Bulk Exemption Filings

In some cases, an employer may opt to file an exemption with DFS on behalf of its employees through the Bulk Submission process. Covered Entities must request access to this functionality. If a Notice of Exemption is filed on your behalf, you will receive an email from DFS confirming the filing. The email will include a receipt number as well as list the exemption(s) filed. It is the licensed person's responsibility to update DFS if their exemption status changes due to a change in employment or any other factor.

Changing or terminating a filed exemption

After an initial Notice of Exemption is filed it can be amended or terminated through the DFS Cybersecurity Portal. The amendment option should be used when the exempt status changes, but the person or entity remains entitled to an exemption. Amending an exemption will leave at least one exemption in place. Terminating an exemption will cancel all previously filed exemptions, including those filed through the Bulk process.

What to File if Licensed by DFS but not Currently Working in Field

500.19(c) applies to any regulated entity or licensed person that does not maintain any Information Systems and does not possess any Nonpublic Information. People who are currently licensed but not actively utilizing such license may fall into this category provided they are not maintaining nonpublic information concerning former or potential consumers or otherwise maintaining information or systems covered by the regulation. This is a partial exemption and still requires that the covered entity or licensed person comply with certain provisions of the Regulation (see chart above). These include the requirement to conduct a Risk Assessment and submit an annual Certification of Compliance to the Superintendent.

Who We Supervise

Institutions That We Supervise

The Department of Financial Services supervises many different types of institutions. Supervision by DFS may entail chartering, licensing, registration requirements, examination, and more.

[Learn More](#)

Department of Financial Services

About Us

[Our History](#)

[Mission and Leadership](#)

[Careers With DFS](#)

[Procurement](#)

[Advisory Boards](#)

State Laws & Regulations

[State Codes, Rules &](#)

[Regulations](#)

[State Laws \(LBDC\)](#)

[State Bills & Laws \(Senate\)](#)

Website

[Accessibility](#)

[Disclaimer](#)

[Language Access](#)

[Privacy Policy](#)

[Site Map](#)

Language Assistance

[English](#)

[Español](#)

[Kreyòl ayisyen](#)

[Polski](#)

[Русский](#)

[বাঙালি](#)

[中文](#)

[한국어](#)

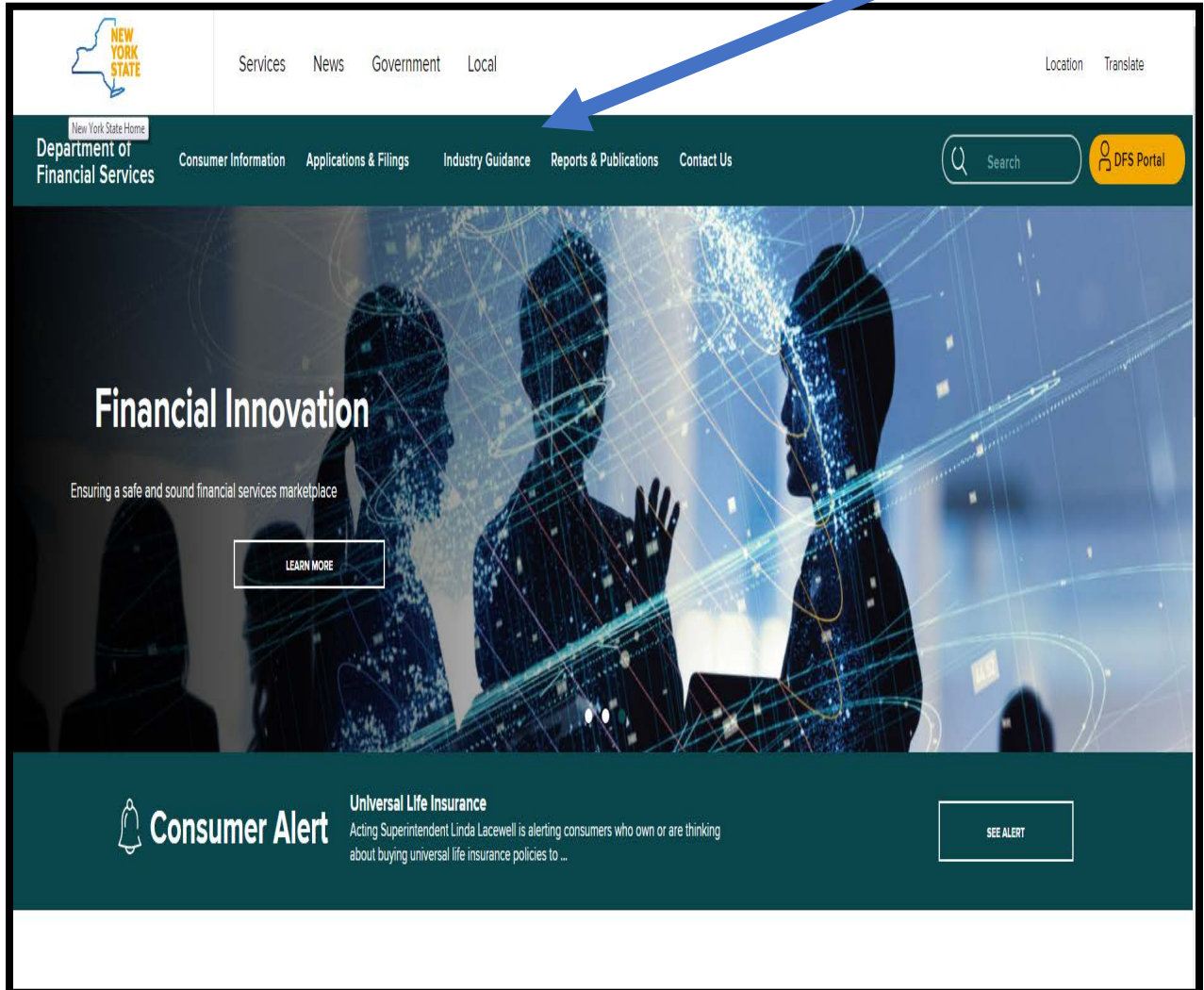
Connect With Us

[!\[\]\(3a9e77fc60554e54e5412caa0cfeb534_img.jpg\) Facebook](#) [!\[\]\(c8c56c3049736ee1c2a2b5340eb11410_img.jpg\) Instagram](#) [!\[\]\(3aedbed8b9acf3a2915697441319daa8_img.jpg\) Twitter](#)

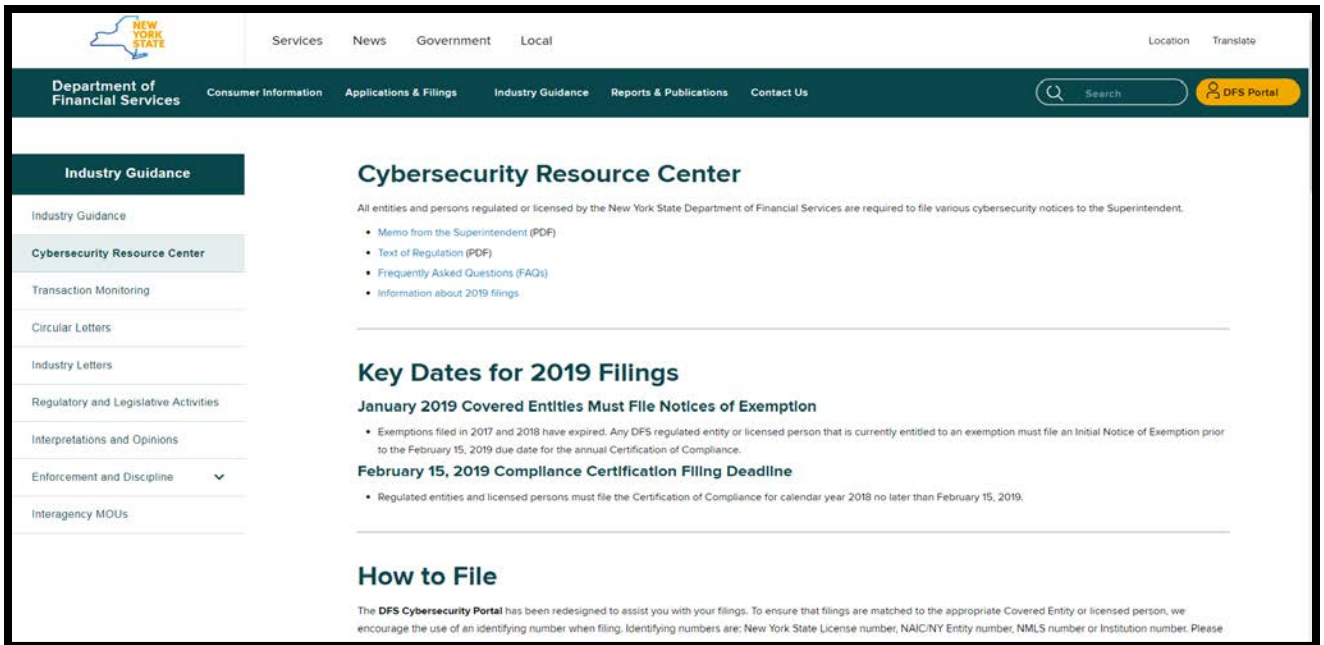
Instructions on How to File Certification of Compliance

The DFS Certification of Compliance is a critical governance pillar for the cybersecurity program of all DFS regulated entities. Prior to **February 15, 2019**, all regulated entities and licensed persons must file a certificate of compliance to the Superintendent covering calendar year 2019 confirming their compliance with the DFS cybersecurity regulation. An entity or individual should only submit a Certification if they were in compliance with all portions of the regulations that apply to that Covered Entity. Even if you filed a Notice of Exemption, you might have to submit a Certification of Compliance to demonstrate that you were in compliance with the portions of the regulation that apply to you.

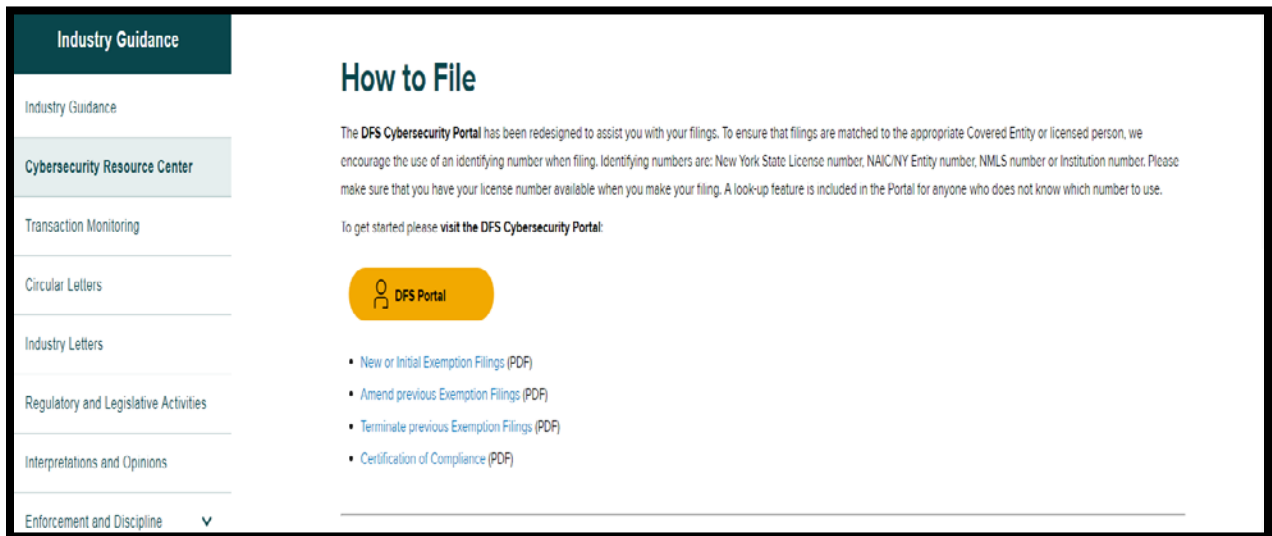
1. First, from the Department of Financial Services webpage (www.dfs.ny.gov), please click on the “Industry Guidance” column.



2. Once in Industry Guidance, click on “Cybersecurity Resource Center” which opens to below:



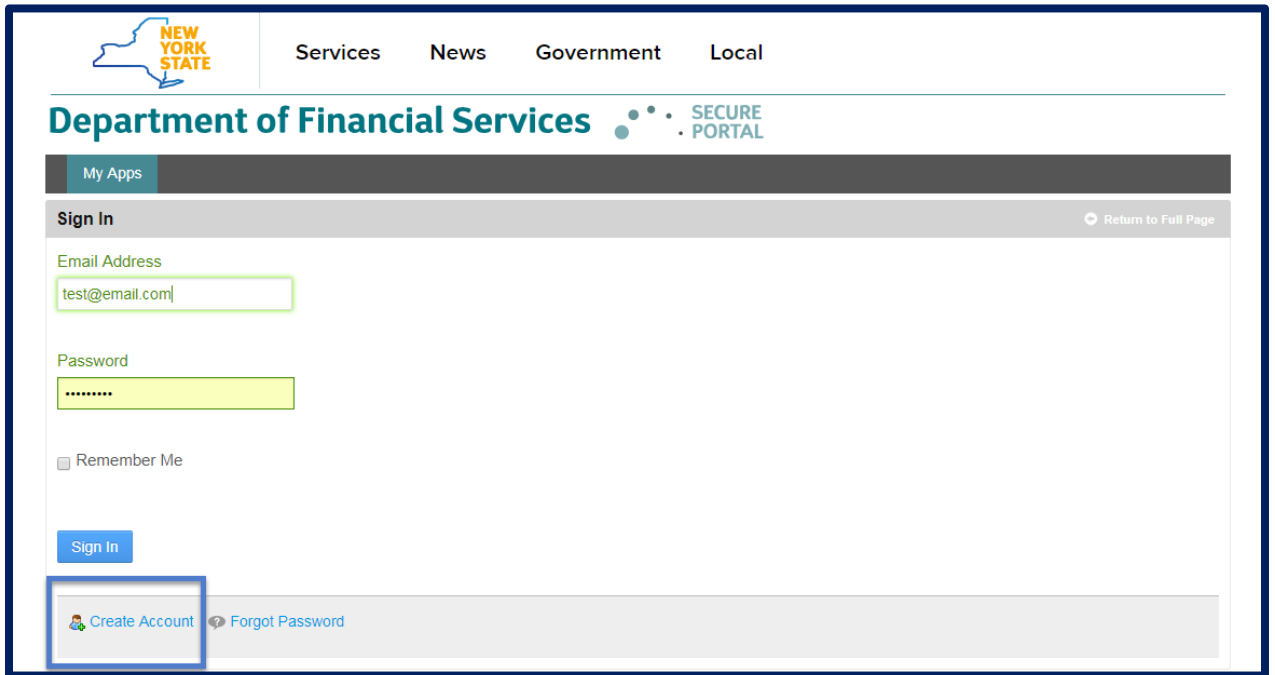
3. Once selected, go to the middle of the page under “Instructions on How to File” you can click on it to access the DFS Cybersecurity Portal. Please note, filing instruction links can be found under “How to File”.



Identify the Filing Entity

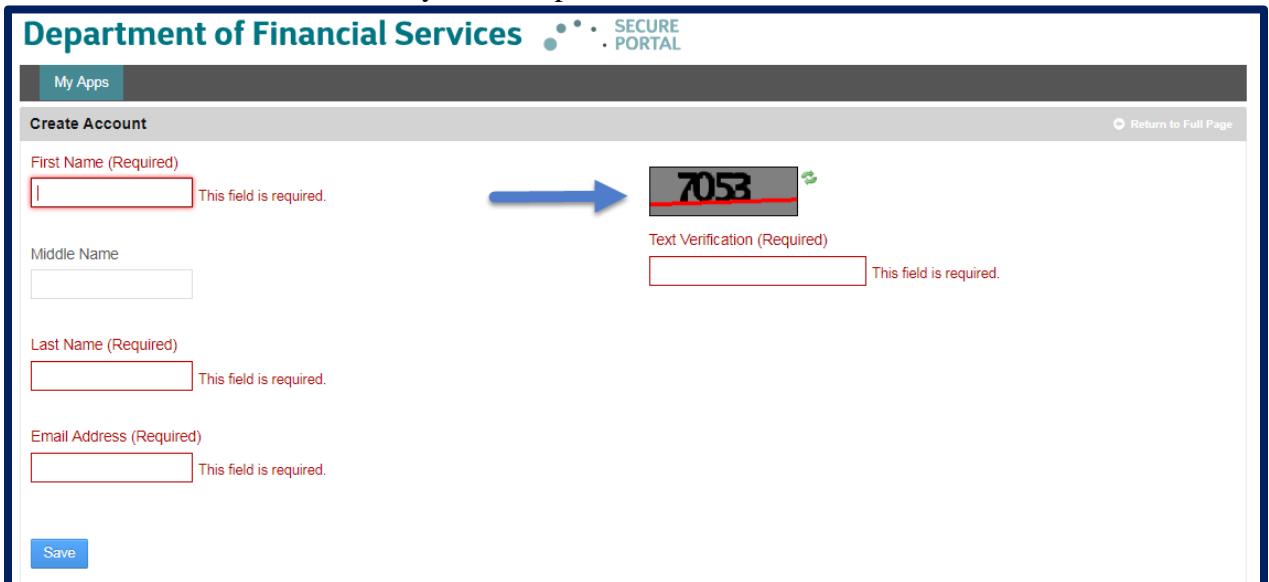
4. Enter your DFS portal account information and select “Sign In.” If you previously made any cybersecurity filing with DFS, the account information you previously used remains the same and you should not create a new portal account. All prior filings are associated with your existing account and you should use the same account.

If you have never created a DFS portal account, you will need to create a new account by selecting “Create Account”. Please refer to the details in the next step for creating a new account.



The screenshot shows the top navigation bar with the New York State logo and links for Services, News, Government, and Local. Below this is the Department of Financial Services logo and the SECURE PORTAL logo. A dark grey bar contains the text "My Apps". The main content area is titled "Sign In" and includes a "Return to Full Page" link. There are input fields for "Email Address" (containing "test@email.com") and "Password" (masked with dots). A "Remember Me" checkbox is present. A blue "Sign In" button is located below the password field. At the bottom of the sign-in section, there are two links: "Create Account" (with a person icon) and "Forgot Password" (with a key icon). The "Create Account" link is highlighted with a blue rectangular box.

5. Skip to Step 9 if you already have an account. After clicking “Create Account”, you will be prompted to enter information required to create a DFS portal account. The “Text Verification” on the right side of the screen will be unique with each attempt to create an account. Select “Save” to create your DFS portal account.



The screenshot shows the "Create Account" page. It features a "Return to Full Page" link in the top right. The form includes several required fields: "First Name (Required)", "Middle Name", "Last Name (Required)", and "Email Address (Required)". Each of these fields is currently empty and has a red border with the text "This field is required." below it. To the right of the "First Name" field, there is a blue arrow pointing to a grey box containing the text "7053" and a green checkmark icon. Below this box is the label "Text Verification (Required)" and an empty input field with a red border and the text "This field is required." below it. At the bottom left of the form is a blue "Save" button.

After selecting “Save”, a confirmation message as shown below will be displayed. Use the password sent to the email address you entered in the prior screen to sign in.

NEW YORK STATE

Services News Government Local

Department of Financial Services SECURE PORTAL

My Apps

Sign In [Return to Full Page](#)

Thank you for creating an account. Your password has been sent

Email Address This field is required.

Password

Remember Me

Sign In

[Create Account](#) [Forgot Password](#)

6. Upon logging in, you will find the landing page shown below.

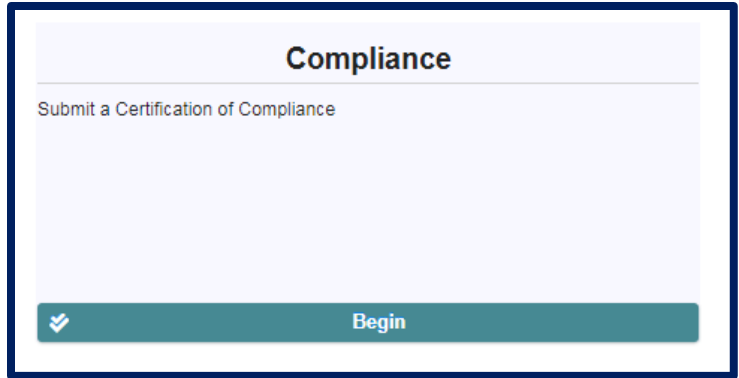
Department of Financial Services SECURE PORTAL

My Apps Cybersecurity

NYS DFS CyberSecurity 23 NYCRR 500 Regulation

Exemption	Compliance	Event
Perform actions related to your entity's NYS DFS cybersecurity regulation exemption status. <ul style="list-style-type: none">File new Notice of ExemptionAmend previously filed Notice of ExemptionTerminate previously filed Notice of Exemption	Submit a Certification of Compliance	Submit Notice of a Cybersecurity Event
Begin	Begin	Begin New
Begin Bulk Exemption		

7. To start a Notice of Compliance Filing, please select “Begin” under the Notice of Compliance banner. You will need to file a Certification of Compliance on an annual basis, by February 15.



8. After clicking Begin, you will need to select the license number that you will be using to identify the regulated company or licensed person for whom you are filing. Please select your NY State License Number, NAIC/NY Entity Number, NMLS Number or Institution Number.

Please note, to facilitate ease of use, DFS allowed the use of different types of license numbers to enable users to identify themselves by various means. The portal includes recommendations for each type of license number. However, most regulated entities and licensed persons have more than one type of license number and the system will accept the filing using any of these types provide you identify the type of number being used. For example, if your company has both an NMLS number and a NYS License number, you can

use either to identify yourself in the portal. If you do not know your entity's number, then please select "Help me find my entity" (Skip to Step 12 for further instructions).

9. If you already know your license number, then you will land on the page below.

Enter Entity Information

Please provide your entity's NYS License #:

[Help me find my entity](#)

10. Please enter your number and click "Search". A message that an entity or individual has been found and the name of the individual or entity will appear in the box; please verify that the information is accurate. If accurate, click next at the bottom right of the screen and skip to step 14.

The following entity or individual has been found, and if you are filing on their behalf, you may continue by clicking 'Next'. Please carefully review the entity information listed below to ensure you select the correct information.

NAME WILL APPEAR HERE

[Help me find my entity](#)

11. If your identifying number is incorrect you will receive the following error message.

Please provide your entity's NYS License #:

No entity or License # could be found which matched your entry.

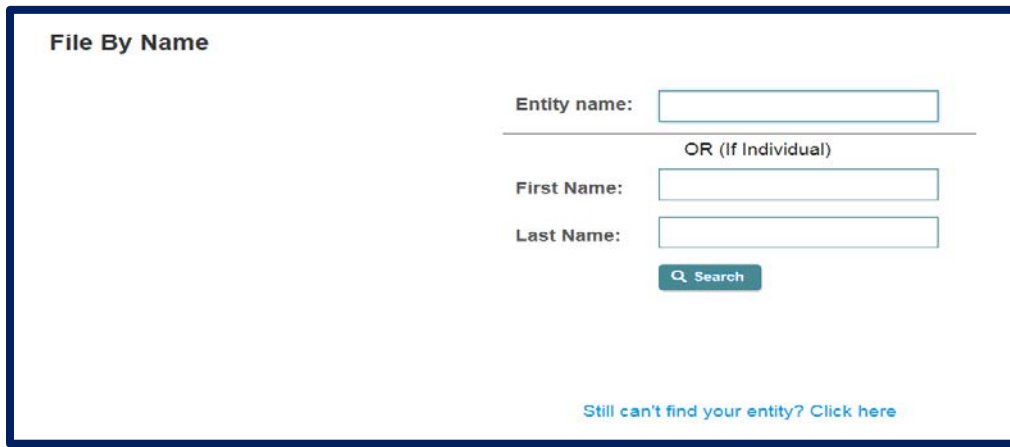
12. If you receive an error, please check your number was entered correctly and search again if possible. If you do not know your number, please select "Help me find my entity" located at the bottom left of the page in blue font.

The following entity or individual has been found, and if you are filing on their behalf, you may continue by clicking 'Next'. Please carefully review the entity information listed below to ensure you select the correct information.

NAME WILL APPEAR HERE

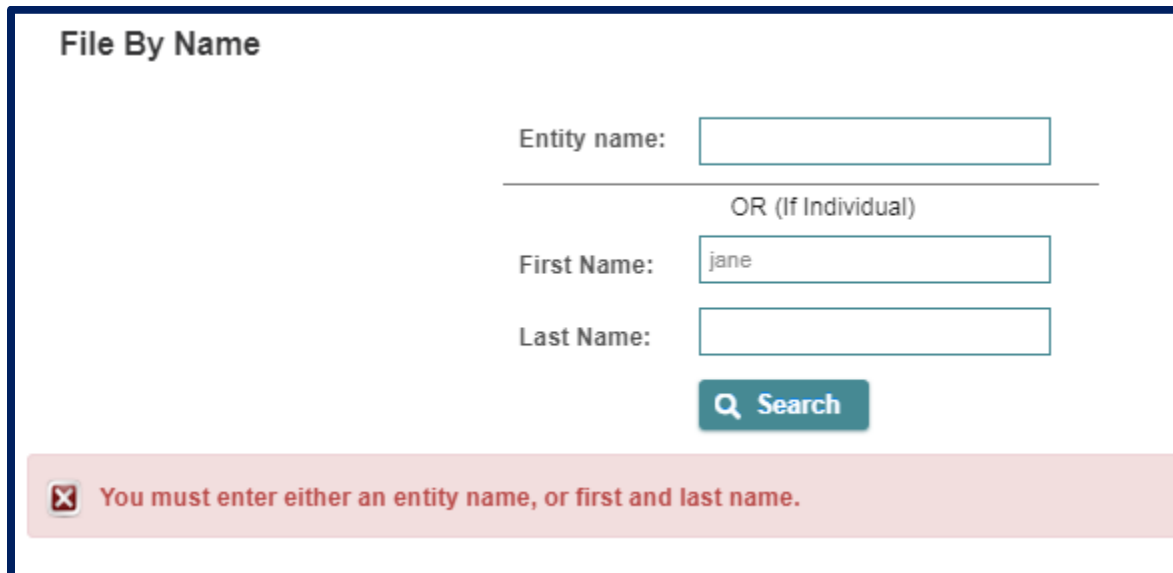
[Help me find my entity](#)

13. Once you select “Help me find my entity” you will see this screen, and you will be able to enter information (your entity name or individual name- including both first name and last name) which will prompt a search for your license number.



The screenshot shows a search form titled "File By Name". It features three input fields: "Entity name:", "First Name:", and "Last Name:". A horizontal line separates the "Entity name" field from the "First Name" and "Last Name" fields. Below the "First Name" field, the text "OR (If Individual)" is displayed. A "Search" button with a magnifying glass icon is located below the "Last Name" field. At the bottom of the form, there is a link that says "Still can't find your entity? Click here".

Note, when searching as an individual, if you do not enter the first and last name you will receive this error message:



The screenshot shows the same "File By Name" search form as above, but with an error message displayed at the bottom. The "Entity name" field is empty. The "First Name" field contains the text "jane". The "Last Name" field is empty. The "Search" button is visible. The error message is: "You must enter either an entity name, or first and last name." The message is preceded by a red square icon containing a white 'X'.

Once you enter your entity information in the Entity name box, then click “Search”, results will appear in blue, which specify the entity name(s) and license number(s) (see example below). Please select the name that matches you or your entity. The name you selected will display in the upper right corner of the screen. You can skip to Step 14.

File By Name

Entity name: All or part of the name

OR (If Individual)

First Name:

Last Name:

[Q Search](#)

Please carefully review the search results before making a selection

Fake Companay Name NYS License #: #####	Fake Companay Name NYS License #: #####	Fake Companay Name NYS License #: #####
Fake Companay Name NYS License #: #####	Fake Companay Name NYS License #: #####	

Showing 5 results

[Still can't find your entity? Click here](#)

14. If you are still unable to find your entity, please click on “Still can’t find your entity?”. By clicking and moving to this page, you will be able to manually enter more detailed information to make your filing. While filing by name is possible, it will not result in your filing being automatically associated with your license record. We may contact you for further information to confirm your license. You may also get notice of delinquency and missing filings until your Notice of Exemption (if applicable) has been associated with your record.

File By Name

Filing by name will require you to provide the additional information below:

Entity or First Name: *	<input type="text"/>
Last Name (required for individuals):	<input type="text"/>
Employed by (required for individuals):	<input type="text"/>
Social Security or Tax ID Number: *	<input type="text"/>
Home Address (required for individuals):	<input type="text"/>
Work or Office Address: *	<input type="text"/>
DOB (required for individuals):	<input type="text"/>
Type of license or field of business: *	<input type="text"/>
Phone Number: *	<input type="text"/>

Back

Submit

Filing a Certification of Compliance

15. Regulated entities and licensed persons must file a Certification of Compliance to the Superintendent covering calendar year 2019 confirming compliance with 23 NYCRR 500. This certification can be made by the Board of Directors, a Senior Officer, or in the case of an individual licensed person, by self. Please indicate who is making the certification for the cybersecurity program.

Certifications by the Board: This option can be used for certifications made by the governing body of any type of corporate body including corporations, partnerships, or any other formations. The certification should be made by the highest governing body, irrespective of whether it is called the “Board of Directors.” When completing the certification for the Board or equivalent governing body, please indicate the name of the Board, partner or committee member(s) who participated in the decision in the first box. In the field for title, please indicate the title(s) of these individuals (i.e., directors, partners, or other applicable title). Please indicate a single email address that can be used for communications with the Board about the certification to certify compliance.

Find My Entity Find My Entity (Cont) **Certification Detail** Signature Done

Certification of compliance reviewed by:

Board of Directors
 Senior Officer(s)
 Self (if filing on behalf of your own individual license)

Name(s) of the Board member(s) certifying Compliance

Title(s)

Email for Board

Covered Entity Tax ID Number

Date of the Board Resolution Compliance Finding

For the year ended (year for which Board Resolution of Compliance Finding is provided)

< Back Next >

16. **Certifications by Senior Officer(s):** This option can be used for certifications made by the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity. When completing the certification for a Senior Officer(s), please indicate the name(s) of the Senior Officer(s) who participated in the decision in the first field. In second field please indicate the title(s) of these individuals. Please indicate a single email address that can be used for communications with the Senior Officers(s) about the certification.

Find My Entity Find My Entity (Cont) **Certification Detail** Signature Done

Certification of compliance reviewed by:

Board of Directors
 Senior Officer(s)
 Self (if filing on behalf of your own individual license)

Name(s) of the Board member(s) certifying Compliance

Title(s)

Email for Board

Covered Entity Tax ID Number

Date of the Board Resolution Compliance Finding

For the year ended (year for which Board Resolution of Compliance Finding is provided)

< Back Next >

17. **Certifications by Individual Licensees:** Self can be used if you are filing for your own individual license. If you are not an entity, but an individual and are filing for a license that you hold for yourself, then select this option.

Find My Entity Find My Entity (Cont) **Certification Detail** Signature Done

Certification of compliance reviewed by:

Board of Directors Senior Officer(s) Self (if filing on behalf of your own individual license)

Name of person self-certifying

Title

Email of person self-certifying

Covered Entity Social Security Number or Tax ID Number

Date of the Self-determination Compliance Finding

For the year ended (year for which Resolution of Compliance Finding is provided)

< Back Next >

18. The signature tab should be completed by the person making the filing in the cybersecurity system.

Name of person submitting certification:

Title of person submitting certification:

Phone:

Email:

19. You will also need to check the box at the bottom of the screen in which you will swear or affirm that you have the authority to submit this certification. After checking the affirmation box, please click “Submit”.

I swear or affirm that I am authorized to submit this Certification of Compliance on behalf of , and that the information herein is accurate. By checking this box, I understand and agree that I am the named person above, that I am electronically signing and filing this Certification of Compliance, and that I agree to the language as stated above.

20. Once your Certification of Compliance has been filed, you will move to the “Done” tab, and you will see a Success message indicating that you have completed your Cybersecurity Certification of Compliance filing (*Appendix A of the Regulation*). Please print/save a copy for your records as it also includes a receipt number which you may need to reference if questions arise. You will also receive an email with this information. If you filed a

Certification on behalf of Senior Officers or Board of Directors, then confirmation of filing will also be sent to the email address provided for the Board of Directors of Senior Officer(s).

[Find My Entity](#) [Find My Entity \(Cont\)](#) [Certification Detail](#) [Signature](#) [Done](#)

Success

You have successfully submitted your Cybersecurity Certification of Compliance form.
Receipt number: C-2018-8002

The Board of Directors of YOUR ENTITY NAME certifies:

(1) YOUR NAME has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary.

(2) To the best of YOUR NAME's knowledge, the Cybersecurity Program as of 12-04-2018 for the 2018 year ended complies with 23 NYCRR Part 500.

Signed by
Name: YOUR NAME
Date: Mon Dec 17 17:10:30 EST 2018

Please note: Covered Entities are required to maintain all documents that support this filing.

For support regarding the submission of your Cybersecurity documents and filings, please contact:
CyberRegComments@dfs.ny.gov

21. Once these steps are completed, you have successfully submitted a Certification of Compliance.



Industry Guidance

23 NYCRR Part 500 - Cybersecurity

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. If a Covered Entity ceases to qualify for an exemption under Section 500.19, how should the Covered Entity notify the Department?

If a Covered Entity ceases to qualify for a previously claimed exemption, the Covered Entity should, as soon as reasonably possible, notify the Department through the DFS Web Portal. The Covered Entity will terminate his previously filed exemption, which will supersede any previous filings. The Department will note that, under Section 500.19(g), if a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, “such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of” 23 NYCRR Part 500. Please note that the Department might require a Covered Entity to periodically refile their exemptions to ensure that all Covered Entities still qualify for the claimed exemption.

2. How must a Covered Entity address cybersecurity issues with respect to Utilization Review (“UR”) agents?

When a Covered Entity is using an independent UR agent, that Covered Entity should be treating them as Third Party Service Providers (“TPSP”). Since UR agents will be receiving Nonpublic Information from that Covered Entity, that Covered Entity must assess the risks each TPSP poses to their data and systems and effectively address those risks. The Covered Entity will ultimately be responsible in ensuring that their data and systems are protected.

3. Can the same entity be a Covered Entity, an Authorized User, and a Third Party Service Provider?

Yes. Depending on the facts and circumstances, the same entity can be a Covered Entity, an Authorized User, and a Third Party Service Provider.

This is common in the case of independent insurance agents. For example, a DFS-licensed independent agent that works with multiple insurance companies is a Covered Entity with its own obligation to establish and maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of its Information Systems and Nonpublic Information. See 23 NYCRR 500.02.

In addition, when the independent agent holds or has access to any Nonpublic Information or Information Systems maintained by an insurance company with which it works (for example, for quotations, issuing a policy or any other data or system access), the independent agent will be a Third Party Service Provider with respect to that insurance company; and the insurance company, as a Covered Entity, will be required under 23 NYCRR 500.11 to have written policies and procedures to ensure the security of its Information Systems and Nonpublic Information that are accessible to, or held by, the independent agent (including but not limited to risk based policies and procedures for minimum cybersecurity practices, due diligence processes, periodic assessment, access controls, and encryption).

Further, an independent agent will also be an Authorized User if it participates in the business operations, and is authorized to use any Information Systems and data, of an insurance company that is a Covered Entity. In such a case, the insurance company must implement risk-based policies, procedures and controls to monitor the activities of the independent agent, as more fully described in 23 NYCRR 500.14.

It is also noted that, like any other Covered Entity, an insurance company may also be a Third Party Service Provider and/or Authorized User with respect to another Covered Entity, including an independent insurance agent.

In all events, each Covered Entity is responsible for thoroughly evaluating its relationships with other entities in order to ensure that it is fully complying with all applicable provisions of 23 NYCRR Part 500.

4. If I have a limited exemption, what provisions of the regulation do I still need to comply with?

Please see charts.

Exemption	Exempt From	Still Required
500.19 (a) (1) Fewer than 10	500.04- Chief Information Security Officer	500.02- Cybersecurity Program 500.03- Cybersecurity Policy

employees working in NYS	500.05- Penetration Testing and Vulnerability Assessments	500.07- Access Privileges 500.09- Risk Assessment 500.11- Third Party Service Provider Security Policy
500.19 (a) (2) Less than \$5 million in gross annual revenue	500.06- Audit Trail 500.08- Application Security 500.10- Cybersecurity Personnel and Intelligence	500.13- Limitations on Data Retention 500.17- Notices to Superintendent 500.18- Confidentiality
500.19 (a) (3) Less than \$10 million in year-end total assets	500.12- Multi-Factor Authentication 500.14- Training and Monitoring 500.15- Encryption of Nonpublic Information 500.16- Incident Response Plan	500.19- Exemptions 500.20- Enforcement 500.21- Effective Date 500.22- Transitional Periods 500.23- Severability

Exemption	Exempt From	Still Required
500.19 (c) Does not control any information systems and nonpublic information	500.02- Cybersecurity Program 500.03- Cybersecurity Policy 500.04- Chief Information Security Officer 500.05- Penetration Testing and Vulnerability Assessments	500.09- Risk Assessment 500.11- Third Party Service Provider Security Policy 500.13- Limitations on Data Retention
500.19 (d) Captive insurance companies that do not control nonpublic information other than information relating to its corporate parent company	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 500.16- Incident Response Plan	500.17- Notices to Superintendent 500.18- Confidentiality 500.19- Exemptions 500.20- Enforcement 500.21- Effective Date 500.22- Transitional Periods 500.23- Severability

5. How must a Covered Entity address cybersecurity issues with respect to a Bank Holding Company (“BHC”)?

Under 23 NYCRR Part 500, the Covered Entity is responsible for compliance with respect to its Information Systems. Therefore, it must evaluate and address any risks that a BHC (or other affiliate of the Covered Entity) presents to the Covered Entity's Information Systems and/or Nonpublic Information. For example, if a Covered Entity shares its data and systems with a BHC, the Covered Entity must ensure that such shared data and systems are protected. Specifically, the Covered Entity must evaluate and address in its Risk Assessment, cybersecurity program and cybersecurity policies the risks that the BHC poses with respect to such shared Information Systems and/or Nonpublic Information. In the same manner, a Covered Entity must also evaluate and address other cybersecurity risks that a BHC may pose to it. A Covered Entity will ultimately be held responsible for protecting its Information Systems and Nonpublic Information that are shared with a BHC or that otherwise may be subjected to risk by a BHC. Other regulatory requirements may also apply, depending on the individual facts and circumstances.

6. Can a Common Trust Fund (“CTF”) that is administered by another Covered Entity rely on the cybersecurity program of that Covered Entity?

A CTF that is administered by another Covered Entity can rely on the cybersecurity program of that Covered Entity, as long as that cybersecurity program conforms with 23 NYCRR Part 500 and fully protects the CTF. Under these circumstances, the Covered Entity must submit a Certification of Compliance with the Department.

If the CTF is administered by a national bank, then the Department will defer to that bank's primary regulator to ensure that the CTF has a proper cybersecurity program. Further, to protect markets, the Department strongly encourages all financial entities, including CTFs administered by national banks, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500.

7. If I am an individual with no Board of Directors, then who can file my Certification of Compliance?

23 NYCRR 500.01 defines Senior Officer as "the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity..." A Covered Entity is defined as "any Person operating under or required to operate under a licenses, registration, charter, certificate, permit, accreditation or similar authorization under the Banking law, the Insurance law or the Financial Services Law". Individuals filing a Certification of Compliance for their own individual license should file their Certification selecting the self option. When choosing self, you will be able to file for your own individual license and will be acting as a Senior Officer, as defined in the Regulation.

8. Are Exempt Mortgage Servicers Covered Entities under 23 NYCRR 500?

Under N.Y. Bank Law § 590(2)(b-1), an exempt entity will need to prove its "exempt organization" status. Since the notification is not an authorization from the Department, an Exempt Mortgage Servicer, under N.Y. Bank Law § 590(2)(b-1), will not fit the definition of a Covered Entity under 500.01(c). However, Exempt Mortgage Loan Servicers that also hold a license, registration, or received approval under the provisions of Part 418.2(e) are required to prove exemption and comply with regulation. With respect to the DFS cybersecurity regulation, given the ever-increasing cybersecurity risks that financial institutions face, DFS strongly encourages all financial institutions, including exempt Mortgage Servicers, to adopt cybersecurity protections consistent with the safeguards and protections of 23 NYCRR Part 500.

9. Are Not-for-profit Mortgage Brokers Covered Entities under 23 NYCRR 500?

Yes. Not-for-profit Mortgage Brokers are Covered Entities under 23 NYCRR 500. 3 NYCRR Part 39.4(e) provides that Mortgage Brokers "which seek exemption may submit a letter application" to the Mortgage Banking unit of the Department at the address set forth in section 1.1 of Supervisory Policy G 1, "together with such information as may be prescribed by" the Superintendent. As this authorization is necessary for a Not-for-profit Mortgage Broker, it is a Covered Entity under 23 NYCRR 500.

10. Do Covered Entities have any obligations when acquiring or merging with a new company?

Section 500.09(a) states that the "Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations." Furthermore, Section 500.08(b) states that the institution's application security "procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity." As such, when Covered Entities are acquiring or merging with a new company, Covered Entities will need to do a factual analysis of how these regulatory requirements apply to that particular acquisition. Some important considerations include, but are not limited to, what business the acquired company engages in, the target company's risk for cybersecurity including its availability of PII, the safety and soundness of the Covered Entity, and the integration of data systems. The Department emphasizes that Covered Entities need to have a serious due diligence process and cybersecurity should be a priority when considering any new acquisitions.

11. Are Health Maintenance Organizations (HMOs) and continuing care retirement communities (CCRCs) Covered Entities?

Yes. Both HMOs and CCRCs are Covered Entities. Pursuant to the Public Health Law, HMOs must receive authorization and prior approval of the forms they use and the rates they charge for comprehensive health insurance in New York. The Public Health Law subjects HMOs to DFS authority by making provisions of the Insurance Law applicable to them. CCRCs are required by Insurance Law Section 1119 to have contracts and rates reviewed and authorized by DFS. The Public Health Law also subjects HMOs and CCRCs to the examination authority of the

Department. As this authorization is fundamental to the ability to conduct their businesses, HMOs and CCRCs are Covered Entities because they are "operating under or required to operate under" DFS authorizations pursuant to the Insurance Law. Moreover, since these entities have sensitive, private data, their compliance with cybersecurity protection is necessary.

12. 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.

13. 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.

14. 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 will be able to amend from their initial filing through the DFS Web Portal. When accessing the portal, Covered Entities will need to choose the "amend exemption" option and file an updated exemption by selecting the exemptions that they still qualify for. 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 amend their Notice of Exemption with the correct information. Please note that the Department might require a Covered Entity to periodically refile their exemptions to ensure that all Covered Entities still qualify for the claimed exemption.

The Department also emphasizes that Notices of Exemption should be filed electronically via the [DFS Portal](#). 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.

15. 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.

16. 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.

17. 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).

18. **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.

19. **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 are any changes, the entity will be able to add and terminate exemptions 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.

20. **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.

21. 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 the DFS 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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).

28. 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.

29. 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.

30. 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.

31. 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.

32. 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 considered applicable for purposes of a certification under 23 NYCRR 500.17(b).

33. 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.

34. 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.

35. 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 [as instructed](#). 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.

36. 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.

37. 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.

Who We Supervise

Institutions That We Supervise

The Department of Financial Services supervises many different types of institutions. Supervision by DFS may entail chartering, licensing, registration requirements, examination, and more.

[Learn More](#)

Department of Financial Services

About Us

[Our History](#)

[Mission and Leadership](#)

[Careers With DFS](#)

[Procurement](#)

[Advisory Boards](#)

State Laws & Regulations

[State Codes, Rules &](#)

[Regulations](#)

[State Laws \(LBDC\)](#)

[State Bills & Laws \(Senate\)](#)

Website

[Accessibility](#)

[Disclaimer](#)

[Language Access](#)

[Privacy Policy](#)

[Site Map](#)

Language Assistance

[English](#)

[Español](#)

[Kreyòl ayisyen](#)

[Polski](#)

[Русский](#)

[বাঙালি](#)

[中文](#)

[한국어](#)

Connect With Us

[!\[\]\(06456157f083c12e510a7643240746db_img.jpg\) Facebook](#) [!\[\]\(10b5acb7a11050b73ad3839d5f3700a7_img.jpg\) Instagram](#) [!\[\]\(1f48a7146c45154f3eeacd7baf560ff1_img.jpg\) Twitter](#)