KeepItSafe®

Cybersecurity Requirements for Financial Services Entities

Wide-Reaching, First-in-the-Nation Regulations

Why: In response to increasing and widespread cyber-attack on banks, insurance companies, and other financial services institutions, New York State has passed the most stringent cybersecurity requirements known to date. The New York Department of Financial Services (NYDFS) has set new guidelines for cybersecurity practices for the state's financial services industry by passing 23 NYCRR Part 500, also referenced as the NY Cyber Rules.

"Data breaches in New York State were up 40% in 2016"

— NY Attorney General

Who: Broadly speaking, the 23 NYCRR 500 applies to any organization that falls under the jurisdiction or is required to operate under NYDFS licensure, registration, charter, permit, or accreditation, including unregulated third-party service providers. There are exemptions for entities with fewer than 10 employees, less than $5 million in gross annual revenue for three years, or less than $10 million in year-end total assets, but they still must comply with some regulations.

When: The NYDFS enacted regulations on March 1, 2017, and covered entities are required to submit an annual written statement (to the superintendent) covering the prior calendar year certifying they are in compliance.

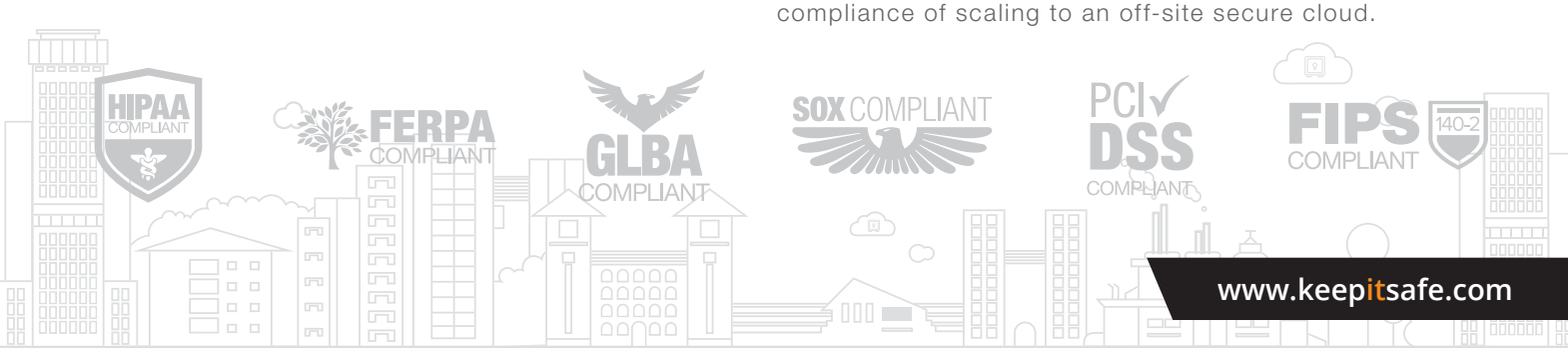
Required Annual Certifications of Compliance By Feb 15, 2018

What: The NYDFS regulations require covered entities to establish a cybersecurity risk program led by a CISO, while documenting their cybersecurity policies and procedures with oversight of third-party service provider management to protect non-public data. Specific requirements include:

- Risk assessments
- Apply written policies and procedures
- Disaster-recovery planning
- Multi-factor authentication
- Penetration testing and assessments
- Audit trail and management
- Privileged access management
- Application security
- Assess third-party security policies
- Limitation of data retention
- Training and monitoring of end users
- Encryption of nonpublic information
- Incident response plan

Where: New York's regulations are likely the opening salvo in what will be a succession of regulations surrounding data protection and application cybersecurity. The federal government may follow in the footsteps of New York and adopt its own framework, while other countries will continue to introduce regulatory frameworks, e.g., the General Data Protection Regulation (GDPR) in Europe.

How: The good news: these regulations will help reduce the risk of attacks, including the risk of data breaches or data loss from insider threats, negligence, ransomware, hardware failures, and natural disasters. KeepItSafe's Cloud Collection of global cloud data availability solutions is uniquely positioned to help your organization with seamless, go-to data protection answers that meet the enhanced data-security compliance of scaling to an off-site secure cloud.



Adoption Timeline

of Part 500 of Title 23 of the NYCRR

New York State Department of Financial Services

2017

March 1st

Section 500.20 Enforcement
The new Part 500 of Title 23 of the Offical Compilation of Codes, Rules and Regulations of the State of New York takes effect.

August 28

Section 500.22 Transitional Periods
Covered Entities shall have 180 days from the effective date of Part 500 to comply with the requirements set forth in this Part, except as otherwise specified.

2018

February 15

Section 500.11 Third Party Service Provider Security 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.

March 1

Section 500.04(b) Chief Information Security Officer
Appoint a CISO responsible for a cybersecurity policy and annually report on the cybersecurity program and risks.

Section 500.05 Penetration Testing and Vulnerability Assessments
Monitor and test on an ongoing basis the effectiveness of the cybersecurity program with annual penetration testing and bi-annual vulnerability assessments.

Section 500.09 Risk Assessment
Conduct periodic risk assessments of information systems and update systems as necessary to protect nonpublic information.

Section 500.12 Multi-Factor Authorization
Implement multi-factor or risk-based authentication to protect against unauthorized access.

Section 500.14(b) Training and Monitoring
Provide regular relevant cybersecurity awareness training for all personnel.

September 1

Section 500.22 Transitional Periods
Entities shall comply with the requirements of section 500.11 of this Part within two years of the effective date.

2019

March 1

Section 500.06 Audit Trails
Maintain financial materials and audit trails for three to five years.

Section 500.08 Application Security
Implement written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications.

Section 500.13 Limitations on Data Retention
Place limitations on data retention that is no longer necessary far operational purposes.

Section 500.14(a) Training and Monitoring
Engage systems to monitor user activity to detect unauthorized access.

Section 500.15 Encryption of Nonpublic Information
Initiate encryption of non-public information that is stored or transmitted.

"Losses from breaches now exceed $400 million annually"

— Data Breach Investigations Report, Verizon, April 2015

Key Dates for Financial Services Cyber Security Regulations

If you are a financial institution such as a bank or investment firm, you know that protecting the security and privacy of your financial data is a major responsibility. The New York Department of Financial Services (NYDFS) enacted mandatory cybersecurity requirements (available here) on March 1, 2017. As of August 28, 2017, 23 NYCRR Part 500 requires all NYDFS covered entities to be compliant, unless exempted. Covered entities will have until February 15, 2018, to self-certify that all requiremen0ts have been met.

Cloud Pedigree and Industry-Compliant

The recent severity of attacks and resulting breaches pose a threat to the economy as well as to national security. Since the NY Cyber Rules affect nearly every aspect of IT security, many affected institutions will still have challenges to implement an effective program within the required timelines. The 23 NYCRR Part 500 requirement will have wide-ranging effects on banks, insurance companies, and financial services companies licensed in New York, along with ancillary third-party service providers such as law firms, accounting firms, consulting firms, and commercial and residential real estate financing professionals — such as mortgage brokers and servicers. The KeepItSafe® team is available to provide secure, data-protection best practices in cybersecurity, especially when it comes to third-party backup and cloud provider regulations, as mandated by the NYDFS.

Frequent Asked Questions

As compliance deadlines draw closer, financial institutions should review all of the FAQs (available here) to confirm that they have aligned their policies, procedures, and practices with the NYDFS interpretation of the regulations. Below is a list of the new FAQs and summaries of each entry:

When is an unsuccessful attack a "Cybersecurity Event" under the reporting requirements of 23 NYCRR Section 500.17(a)(2)?

Organizations should use good judgment when deciding whether to report unsuccessful attacks. The NYDFS encourages entities to assess whether the response to an incident requires measures beyond their usual procedures, such as attention by senior personnel or adoption of extra steps. The NYDFS does not intend to penalize entities that are acting in good faith.

Are the New York branches of out-of-state domestic banks required to comply with 23 NYCRR Part 500?

The home state of a state-chartered bank is primarily responsible for its supervision, and NYDFS defers to the home state supervisors in the examination of New York branches, but encourages all financial institutions to adopt cybersecurity protections.

How must a covered entity address cybersecurity issues with respect to its subsidiaries and other affiliates?

In conducting the required risk assessment and creating its cybersecurity program and policy, a covered entity must address the risks posed by their subsidiaries and affiliates.

If a covered entity qualifies for a limited exemption, does it need to comply with 23 NYCRR Part 500?

A covered entity must still comply with the applicable provisions listed in the designated exemption. The exceptions were designed to be tailored for particular circumstances, not to allow covered entities to avoid all cybersecurity requirements.