proofpoint.

SOLUTION BRIEF

Proofpoint and New York State Department of Financial Services Cybersecurity Regulation 23 NYCRR 500

To address the importance of security in financial services companies and the ever-increasing threats they face, the New York State Department of Financial Services (DFS) issued Regulation 23 NYCRR 500 (or Reg 500) in March 2017. This includes a comprehensive set of cybersecurity regulations that applies to any institution regulated by the New York State DFS.

If this applies to your organization, you must meet all the regulation requirements. They were designed to ensure that you improve your cybersecurity posture and increase the data protection and privacy for your customers. In all, its 21 provisions give you guidelines and standards on how you must develop a thorough cybersecurity program and a process to comply and disclose incidents.

According to Reg 23 NYCRR 500, your comprehensive cybersecurity program must include:

- One or more written security policies
- A risk assessment
- Implementation of security and archiving applications
- Security awareness training
- Encryption
- Multi-factor authentication
- Testing and auditing
- Certification
- Filing of incident reports
- And more

As of March 2019, all the regulation's requirements are in effect. And regardless of your compliance efforts, there will always be differences in interpretation from auditors or internal compliance groups regarding the ongoing strength and operationalization of NYDFS CRR 500.

The regulation has grown in popularity and has ushered in a growing wave of other state-level measures and guidance. It has also led to growing expectations for federal-level (Federal Trade Commission) privacy and security compliance regulations that impact financial services. For example, the NAIC Insurance Data Security Model Law closely mirrors and aligns with much of CRR 500. Another example on the privacy end is the California Consumer Privacy Act (CCPA), effective January 2020. Overall, the respective missions are the same. These all aim to protect financial consumers and markets from fraud.

What Firms Must Comply?

Your organization must comply if it's a state-chartered and non-U.S licensed bank, mortgage company or lender, insurance firm or broker-dealer, or other. The regulation applies to any company that falls under NYDFS jurisdiction with business operations in the state of New York, including both its domestic and international organizations. As noted in the regulation, entities mean, "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."

Your firm may be exempt from some of the requirements. The exceptions include firms with less than 10 employees, less than $5M in New York-based revenue in each of the past three years, or less than $10M in total year-end assets.[1]

1 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.

Potential Penalties

Historically, NYDFS has imposed fines for compliance failures. Penalties for NYCRR500 could range from a firm having their license revoked to a financial one that could be upwards of $250K and/or 1% of total assets of the bank or subsidiary.

Proofpoint and Title 23 NYCRR 500

The table below highlights the major provisions of 23 NYCRR 500 and how Proofpoint security and compliance solutions and services can help.

Proofpoint Solution Coverage for 23 NYCRR 500 Provisions

NYDFS 23 NYCRR 500 MAJOR PROVISION	PROOFPOINT SOLUTION COVERAGE
Section 500.02 Cybersecurity Program Section 500.02 (A) Use defensive infrastructure and the implementation of policies and procedures to protect Information Systems.	**Section 500.02 Cybersecurity Program** Section 500.02 (A) • Enterprise Protection for Email • Targeted Attack Protection • Proofpoint Cloud Account Security Broker • Threat Response Auto Pull • Internal Mail Defense • Cloud Account Defense • Email Isolation • Email DLP • Email Encryption • CASB • Web Isolation • Digital Risk • Email Fraud Defense • Zero Trust Networking • E-Discovery & Governance • Email Continuity • Proofpoint Security Awareness Training
Section 500.02 Cybersecurity Program Section 500.02 (B) Protect Information Systems, and the Nonpublic Information stored on them from unauthorized access, use or other malicious acts.	**Section 500.02 Cybersecurity Program** Section 500.02 (B) • Enterprise Protection for Email • Data Discover • Proofpoint Cloud Account Security Broker
Section 500.06 Audit Trail Section 500.06 (A)(1) Maintain systems so that financial transactions can be reconstructed.	**Section 500.06 Audit Trail** Section 500.06 (A)(1) Proofpoint Archive, eDiscovery, Supervision and Data Loss Prevention solutions can be used to help reconstruct financial transactions with respect to communications and messaging associated with them.
Section 500.06 (A)(2) Include audit trails designed to detect and respond to cybersecurity events.	Section 500.06 (A)(2) Proofpoint security products have logging capabilities and/or APIs that can used to create audit trails, which can be used to detect and respond to cybersecurity events.

Proofpoint Solution Coverage for 23 NYCRR 500 Provisions, continued

NYDFS 23 NYCRR 500 MAJOR PROVISION	PROOFPOINT SOLUTION COVERAGE
Section 500.06 Audit Trail	**Section 500.06 Audit Trail**
Section 500.06 (B)	Section 500.06 (B)
Maintain records required by section 500.06(A)(1) for not fewer than five years and maintain records required by section 500.06(A)(2) for not fewer than three years.	Archive
Section 500.07 Access Privileges	**Section 500.07 Access Privileges**
Section 500.07	Section 500.07
Limit user access privileges to information systems that provide access to nonpublic information and periodically review such access privileges.	• Proofpoint Meta Networks solutions. • Partner solutions from Okta and Imperva
Section 500.10 Cybersecurity Personnel and Intelligence	**Section 500.10 Cybersecurity Personnel and Intelligence**
Section 500.10 (A)(1)	Section 500.10 (A)(1)
Qualified cybersecurity personnel must be used to manage risks and perform or oversee the performance of core cybersecurity functions specified in 500.02 (1) – (6). The cybersecurity personnel can be employed by the company, an affiliate, or 3rd-party.	Proofpoint Managed Services
Section 500.10 (A)(2)	Section 500.10 (A)(2)
The cybersecurity personnel must be trained on cybersecurity risks on an ongoing basis, and	PSAT for training and PTIS for cybersecurity updates
Section 500.10 (A)(3)	Section 500.10 (A)(3)
steps must be taken to verify that they maintain knowledge on changing cybersecurity threats and countermeasures.	Premium Security Services
Section 500.10 (B)	Section 500.10 (B)
An affiliate or qualified third-party service provider can be utilized to assist in complying with the requirements set forth in Section 500.10, subject to the requirements set forth in section 500.11.	PSAT Managed Services and Premium Security Services
Section 500.12 Multi-Factor Authentication	**Section 500.12 Multi-Factor Authentication**
Section 500.12	Section 500.12
Multi-Factor Authentication (MFA) or Risk-Based Authentication must be used as controls to protect unauthorized access to nonpublic information or information systems. MFA must be utilized for anyone who attempts to access internal networks from an external network, unless the company's CISO has approved the use of reasonably equivalent or more secure access controls.	CASB and Meta Networks can pivot users dynamically to MFA for Risk-Based Authentication due to factors like being a VAP, interaction with sensitive data, or accessing non-public information from external networks. Proofpoint Partner solution from Okta to provide MFA.
Section 500.13 Limitations on Data Retention	**Section 500.13 Limitations on Data Retention**
Section 500.13	Section 500.13
Nonpublic information must be disposed of on a periodic basis as it pertains to section 500.01(g)(2)-(3).	Proofpoint Archive retention policy

Proofpoint Solution Coverage for 23 NYCRR 500 Provisions, continued

NYDFS 23 NYCRR 500 MAJOR PROVISION	PROOFPOINT SOLUTION COVERAGE
Section 500.14 Training and Monitoring	**Section 500.14 Training and Monitoring**
Section 500.14 (B)	Section 500.14 (B)
Provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the company in its Risk Assessment.	Proofpoint Security Awareness Training
Section 500.15 Encryption of Nonpublic Information	**Section 500.07 Access Privileges**
Section 500.15 (A)	Section 500.15 (A)
Encryption is required for Nonpublic Information at rest or in transit over external networks.	Email Encryption
Section 500.15 (A)(1) and (A)(2)	Section 500.15 (A)(1) and (A)(2)
To the extent that encryption is infeasible for Nonpublic Information at rest or in transit over external networks, alternative compensating controls can be used, which must be approved by the CISO.	Data Loss Prevention

LEARN MORE

For more information, visit **proofpoint.com**.