

A WithSecure™ Consulting whitepaper



NYDFS 500

Plan for Stronger Cyber Security Compliance

WITH™
secure

NYDFS 500: Plan for Stronger Cyber Security Compliance

The New York State Department of Financial Services (NYDFS) Cybersecurity Regulation enacted in 2017 has resulted in numerous enforcement actions and monetary penalties averaging several million dollars. Amendments to the regulation enacted in November 2023 will present financial institutions operating in New York with even greater challenges in maintaining their compliance.

WithSecure Consulting is pleased to offer thoughts and insights on the NYDFS Regulation for covered entities who are working toward ensuring their compliance with the new requirements.



Background

The NYDFS is a regulatory agency that oversees financial institutions operating in New York. It is responsible for ensuring the safety and soundness of financial institutions, protecting consumers, and promoting the growth of the NY financial services sector. NYDFS Covered Entities include banks, insurance companies, mortgage lenders and other financial institutions.

In March 2017, NYDFS promulgated a Cybersecurity Regulation (23 NYCRR Part 500). The intent was to ensure covered entities establish and maintain strong cyber security practices to protect consumers and the stability of the financial system from the increasing pace of sophistication of cybercriminals targeting the finance industry.

At a high level, the regulation required Covered Entities to perform risk assessments, designate a qualified CISO to implement and enforce a cyber security program and policies, and maintain effective cyber security functions such as identity & access management, third party service provider oversight and incident response. The regulation also required covered entities to notify NYDFS of cyber security incidents within 72 hours of occurrence and to submit an annual certification of their compliance with the regulation.

As of June 2024, at least 16 entities had been impacted by NYDFS enforcement actions which included monetary penalties for violating the Cybersecurity Regulation. As a result of these Enforcement Actions, all entities were required to develop and submit remediation plans the NYDFS and provide on-going progress reports, except one entity which surrendered its license to conduct business in NY and ceased operations. Details of these actions are published on the [NYDFS website](#).

In September 2022, NYDFS published a proposed second amendment to the Cybersecurity Regulation which introduced heightened cyber security requirements. As with the initial regulation, the amendment was opened for public comments and based on this feedback, NYDFS made some changes to the initial draft before finalizing the amendment in November 2023.



Enforcement Actions

Enforcement actions are the legal measures that NYDFS takes against Covered Entities that violate its regulations. Most enforcement actions are based on a consent order which is a legally binding document that outlines the terms and conditions agreed upon by NYDFS and the Covered Entity to settle the matter without going to trial.

A typical Consent Order related to NYDFS 500 describes the cyber security incident or exam deficiencies that led to the action, identifies specific sections of the regulation that were violated, prescribes remedial actions and includes a monetary penalty. Enforcement actions are public records published on the NYDFS website and are usually accompanied by a press release.



WithSecure Consulting analyzed NYDFS enforcement actions related to the Cybersecurity Regulation to gain insight into the types of security incidents that occurred and the sections of the regulation that were found to have been violated.

Key findings from this analysis include:

- Of the 114 enforcement actions issued by NYDFS since 2020, 16 (14%) were related to violations of the Cybersecurity Regulation
- The average Monetary Penalty was almost \$3 million
- The reviewed actions identified 75 separate violations of specific sections of the Cybersecurity Regulation
- Nine actions (56%) included a violation for falsely or improperly certifying compliance with the Cybersecurity Regulation as evidenced by the entity suffering a security breach
- Seven actions prescribed specific remediation requirements
- One action was against an entity not subject to regulation by NYDFS that had experienced a security breach which affected Covered Entities
- The reviewed actions described 17 separate security incidents, with four entities having suffered multiple events
- The security incidents included 15 instances of phishing attacks
- Eight of the security incidents resulted in exposure of non-public information
- Four incidents involved ransomware
- Three incident results in theft of funding with a combined total of \$1,935,000

Factors that led to these penalties included failure to:

- Implement and maintain adequate BCDR policies
- Review user access privileges
- Conduct periodic risk assessments
- Implement procedures for secure application development
- Provide cyber security personnel with sufficient training
- Designate a CISO
- Submit annual certifications of compliance
- Implement and maintain cyber security policies
- Encrypt NPI in transit and at rest
- Implement MFA
- Submit annual written reports to the Board of Directors
- Notify NYDFS of security incidents
- And the catch all: Establish and maintain an effective cyber security program

The lowest penalty for non-compliance was \$150K, however this was for a very small entity. All other penalties were \$1M and above, and the highest was \$8M though this also included fines for non-compliance with AML regulations. The largest penalty which only involved non-compliance with the Cybersecurity Regulation was \$4.25M.

Financial institutions should also note a significant development: NYDFS is shifting from reactive to proactive enforcement of the Cybersecurity Regulation. Before 1Q23, 10 of 11 penalties were due to a cyber security incident, and only one was related to deficiencies NYDFS discovered during an exam; since 1Q23, 4 of 5 penalties were due to exam deficiencies and only one due to a cyber security event. This shift underscores the need for financial institutions to be even more diligent in maintaining compliance to avoid fines.

The Second Amendment

In November 2023, NYDFS enacted a Second Amendment to the Cybersecurity Regulation which added more stringent requirements. According to NYDFS, the amendment is intended to address common cyber weaknesses that they have identified since 2017. In particular, the NYDFS has observed that some regulated entities have failed to:

- Properly implement MFA for remote access by authorized users
- Remediate vulnerabilities in a timely manner
- Replace vulnerable end of life systems
- Secure ports that allow remote access
- Monitor for abnormal system activity
- Secure applications effectively
- Adapt policies and procedures to evolving cyber threats

Top 10 List

WithSecure Consulting believes the following new requirements will be the most impactful to covered entities:

The sections below list noteworthy changes and themes.

1. Timely Vulnerability Remediation
2. Automated Vulnerability Scans and Manual Reviews
3. Asset Inventory
4. Centralized SIEM Solution
5. Endpoint Detection and Response Solution
6. Privileged Access Management Solution
7. BC/DR Plan Development and Maintenance
8. Incident Response and BC/DR Plan Testing
9. Secure Backups and Backup/Restore Testing
10. Annual Independent Audit of the Cybersecurity Program




Class A Companies

The amendment introduces the category 'Class A companies' which are larger institutions subject to heightened requirements. Class A companies are covered entities with at least \$20M in annual revenue in New York -AND- over 2,000 employees -OR- at least \$1B in annual revenue including outside of NY.

Additional requirements for Class A companies:

- Annual Independent Audit of Cybersecurity Program
- Password Policy
- Automated method to block weak passwords
- Privileged Access Management Solution
- Endpoint Detection and Response Solution
- Centralized SIEM Solution



Bar Raisers

Several of the changes "raise the bar" for cyber security regulation, for example:

- Annual Certification of Compliance must be signed by the CEO
- Updated and in-depth requirements for Risk Assessments
- Entities must notify NYDFS and provide justification if they make a ransomware payment
- The Board of Directors (BoD) is responsible for Risk Management Oversight
- The BoD must have cyber security knowledge and expertise
- Social engineering exercises e.g. phishing simulations now required
- BC/DR Plan development and maintenance
- Provide ongoing updates on security incidents to NYDFS and respond to any information requests



New Ground

The amendment includes some new and interesting concepts, such as

- For annual certifications, entities may acknowledge non-compliance with the regulation if they also submit a remediation plan and timeline
- Entities will be considered in violation for "commission of a single prohibited act" including: failure prevent unauthorized access or failure to comply with any section of the regulation for more than 24 hours
- NYDFS identified 15 factors they will take into account when assessing monetary penalties for violations

Conclusion

The cyber security regulatory landscape continues to evolve and NYDFS is at the forefront. Financial institutions operating in New York must meet the highest standards to avoid regulatory action and substantial penalties. Recent amendments to NYDFS 500 are likely to pose challenges for even the most mature cyber security programs.

WithSecure Consulting is committed to supporting organizations in meeting regulatory and other cyber security challenges. Please see below a listing of services offerings which may be of value to organizations in managing compliance with the NYDFS 500 amendment.

Cyber Security Program Design | Security Strategy

Our experts help you design and implement a robust cyber security program that meets the regulation's requirements.

Annual Independent Audit of the Cyber Security Program | Cyber Security Maturity Assessment (CMA)

We conduct thorough cyber security maturity assessments (CMAs) modeled after our proven PCI DSS compliance assessments.

Remediation Plan Development | Security & Risk Management

Following a CMA, we'll help you craft a comprehensive remediation plan to address identified gaps.

Penetration Testing | Security Assurance

We offer penetration testing services to identify and address vulnerabilities in your information systems.

Incident Response Plan Testing | Incident Readiness Exercises

We conduct realistic incident response plan testing exercises to ensure your team is prepared to handle security incidents effectively.

Annual Reporting | Board of Directors Reporting Package

After a CMA, we can help you create a BoD reporting package that meets NYDFS requirements.

Examination Support

We help you throughout the NYDFS examination process, including pre-examination preparation and post-examination support.



Thank you for your interest.

Please contact us for any questions on this article or the NYDFS Cybersecurity Regulation.

Who We Are

WithSecure® Consulting, formerly part of F-Secure Business, is your reliable partner in cyber security.

Businesses, including some of the world's biggest financial institutions, manufacturers, and numerous advanced communications and technology providers, rely on us for cyber security services that protect and enable their operations.

Our consultants partner with enterprises and tech disruptors to build resilience through evidence-based security advice. We have more than 30 years of experience in business centric cyber security assurance services.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.