okta

How to Meet NYDFS Mandates with Identity & Access Management

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

Content

How to Meet NYDFS Mandates with Identity & Access Management

"The financial services industry is a significant target of cybersecurity threats... given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted."

The New York Department of Financial Services

Introduction

Given the advent of new and evolving compliance regulations, including recent landmark mandates from the New York Department of Financial Services (NYDFS), impacted technology professionals need to ensure that their organizations employ modern solutions that augment the capabilities of traditional Identity and Access Management (IAM).

This white paper is designed for Information Technology (IT) and Information Security (IS) professionals and technology-focused executives, and reviews the NYDFS IAM-related mandates and their impact on the organizations that are subject to them ("Covered Entities"), as well as specific solutions from Okta, including Adaptive MFA and Lifecycle Management, that can help Covered Entities ensure compliance with the new NYDFS mandates. Please note that this white paper, while discussing legal topics and analyzing certain regulations, does not constitute legal advice. If you or your organization needs legal advice regarding the topics covered here, please contact an attorney.

All content included by Okta in this white paper is provided for informational purposes only.

On March 1, 2017, the NYDFS Cybersecurity Requirements went into effect as defined under 23 NYCRR Part 500. The new rule applies to nearly 1,900 banking and other financial institutions, whose collective assets total more than $2.9 trillion, and all insurance companies that do business in New York state, which includes nearly 1,700 insurance companies whose collective assets exceed $4.2 trillion. The new mandates affect licensed lenders, state-chartered banks, trust companies, service contract providers, private bankers, mortgage companies, insurance firms doing business in New York, non-U.S. banks licensed to operate in New York, and many other organizations. NYDFS mandates cast a wide net—far beyond just financial firms operating in New York.

While many of the existing compliance mandates prescribe specific actions or requirements, the NYDFS guidelines focus on a cybersecurity program risk assessment to determine the adequacy of a Covered Entity's best practices and policies to mitigate identified risks. Effective IAM, specifically in the form of Multi-Factor Authentication (MFA) or equivalent measures, is now required by the NYDFS. Specifically, section 500.1 defines MFA as follows:

> 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.

Additional sections that are pertinent to effective IAM include:

> 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.

NYDFS also describes how each Covered Entity needs to implement and maintain cybersecurity policies. One of the areas explicitly covered as part of the cybersecurity policies relates to access controls and identity management. Covered Entities must prove they have effective IAM measures in place to eliminate or reduce unauthorized access to sensitive information by hackers, phishers, insiders, or third-parties.

The new mandates indicate that the NYDFS views IAM as the first line of defense in protecting vital customer and business information. If a Covered Entity's IAM authorization processes are not well defined, are too permissive, or are ineffectively maintained, other tactics—such as encryption or data breach detection—will not be as effective in accomplishing the goals of the NYDFS cybersecurity guidelines.

Under the new mandates, identity has become an even more critical control point and plays a vital role in preventing credential-related security risks. For many Covered Entities, an improved IAM posture is required to ensure compliance. Implementing MFA, Lifecycle Management and other solutions can help ensure compliance through simplicity for administrators and users, secure authentication across all applications, and extensibility throughout the entire organization and security stack.

The Security Landscape

Cybersecurity attacks have increased dramatically over the past decade and most are related to two key areas of concern for IT and IS professionals:

Weak or Stolen Credentials

Cybersecurity attacks are increasing drastically as organizations expand the use of cloud and mobile apps. For IT and IS professionals, staying ahead of the risks is a difficult and demanding challenge. The Symantec April 2017 Internet Security Threat Report validates that over the last 8 years, more than 7.1 billion identities have been exposed in data breaches. The 2017 Verizon Data Breach Investigation Report documents that more than 80% of data breaches involve stolen or weak identity credentials. Privacyrights.org has reported that over the past few years, 893 publicly acknowledged breaches resulted in over 172 million lost records. This concerning statistic does not include one of the largest breaches reported by credit agency Equifax in September 2017, wherein social security numbers and birth dates for 143 million people were stolen by hackers.

Phishing Attacks

The 2016 Verizon Data Breach Investigation Report also validates that over 90% of phishing attacks target user credentials. These attacks are becoming more frequent and sophisticated and usually entail phishing or spear phishing under the heading of "social engineering." Despite frequent efforts undertaken by organizations to educate users about this threat, credential phishing is still rampant. Simple password protections are no longer adequate. In the typical enterprise, 73% of passwords are duplicates and up to 40 services are often registered to one email account. The average

user only has five passwords for these accounts, which hackers can now easily crack.

The potential for non-compliance with the new mandates has increased dramatically as phishing and other attacks escalate, and as regulated organizations have less control over passwords, mobile devices and networks employed by users. Each time an employee connects to an open network at a local coffee shop, the possibility for a breach that requires notices to affected consumers and certain government bodies occurs. Under 23 NYCRR 500.17(a)(1), this type of data breach constitutes a Cybersecurity Event and must also be reported to the NYDFS.

Given these concerning facts, improving identity validation is now one of the most important tasks that IT and IS professionals can undertake. Implementing effective MFA and Lifecycle Management solutions, such as those from Okta, can help improve your overall cybersecurity and IAM posture while ensuring compliance with the ever-evolving NYDFS regulations.

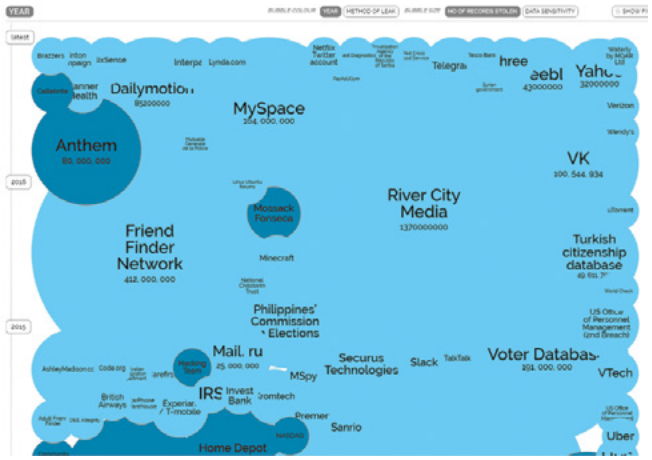
Cyber attacks target credentials

Credential harvesting is the most fruitful tactic for today's threat actors

From 2015 through the present, there were **893 publicly acknowledged breaches** resulting in **172,023,115 lost records**.[4]

In 2016, the average cost of data breach in the USA became **$221 per record**. The average cost of a data breach in 2016 was **$4 million**.[5]

World's Biggest Data Breaches



Selected losses greater than 30,000 records (updated 5th Jan 2017)

Data Security Statutes

Financial, insurance, banking, and related firms typically need to comply with regulatory mandates related to the Federal Trade Commission Act, Gramm-Leach-Bliley, FINRA, PCI DSS, GLBA, and others. These controls have been in place for some time, but the NYDFS determined that most are not adequate or granular enough to deal with escalating security threats. Given the large number of financial firms in the State of New York, the NYDFS created a new, more comprehensive set of regulations they introduced in 2017.

Financial Regulations

Cyber Security

[1] 2017 Verizon Data Breach Investigations Report
[2] 2016 Verizon Data Breach Investigations Report
[3] TeleSign 2016 Consumer Account Security Report
[4] privacyrights.org
[5] The Ponemon Institute, 2016 Cost of Data Breach Study

What is the NYDFS 23 NYCRR Part 500?

According to a recent report from IBM X Force, the average financial services firm experiences 65% more cyberattacks than the typical organization across all industries. With phishing and other security attacks on the rise, the number of attacks against financial services firms increased from 1,310 in 2015 to 1,684 in 2016. In response to these threats, New York became the first U.S. State to propose cybersecurity regulations for financial firms (Covered Entities).

To ensure compliance, the NYDFS provided for a six-month transitional period to allow Covered Entities time to comply. By February 15, 2018, Covered Entities must be able to demonstrate full compliance by submitting annual Certifications of Compliance.

How Will the NYDFS Regulations Impact You?

NYDFS regulations require Covered Entities to comply with the following requirements by the dates indicated. If your firm is a Covered Entity, you must review and understand what's required and ensure you are in compliance. You can find more information on this at 23 NYCRR Part 500.

August 28, 2017

- Establish a cybersecurity program
- Create and follow a set of cybersecurity policies
- Assign an internal CISO or utilize a third-party service provider
- Limit and periodically review user access privileges
- Hire internal or third-party qualified cybersecurity personnel
- Establish a written incident response plan

Definition of Information Systems:

Within the mandates, the NYDFS refers to an Information System that represents "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."

The NYDFS uses this definition to include sensitive data and systems that must be safeguarded against cybercrimes and IAM security threats.

Definition of Nonpublic Information (NPI)

The NYDFS also refers to Nonpublic Information, which means "all electronic information that is not Publicly Available Information" and contains business related information concerning an individual that can be used to identify him/her by name, number, personal mark, or other identifier, in combination with social security number, driver's license number or non-driver identification card number, account number, credit or debit card number, any security code, access code or password that would permit access to an individual's financial account, or biometric records.

The proposed regulations are designed to reduce the risk of data breaches caused by insider threats, ignorance, or unintentional data leakage. As noted in the Introduction, implementing effective IAM is the first line of defense required to protect NPI.

February 15, 2018

- Submit initial certification of compliance

March 1, 2018

- Establish periodic penetration testing and vulnerability assessments
- Conduct periodic risk assessment of information systems
- Use Multi-Factor Authentication or risk-based authentication
- Provide regular cybersecurity awareness training
- Deliver an annual report by the CISO to the board of directors on the cybersecurity program and any risks

September 3, 2018

- Maintain records and audit trails
- Establish and follow guidelines for application security
- Limit data retention and establish proper procedures for safe data disposal
- Monitor and detect unauthorized access of sensitive information
- Encrypt nonpublic data in motion and at rest

March 1, 2019

- Complete creation and application of security policies to third-party providers that have access to data

Definition of Third Party Service Provider(s)

This refers to a Person or Entity that's not an Affiliate of the Covered Entity, provides services to the Covered Entity, and maintains, processes or otherwise is permitted access to NPI through its delivery of services to the Covered Entity. This might include a security consultant or Managed Security Services Provider (MSSP). Any IAM solutions implemented must have the ability to identify third-parties and allow them access only to the NPI relevant to their function. Cybersecurity policies may need to be altered to restrict or narrow access to third-parties if the security assessment shows that it is currently too broad.

Liabilities

The consequences to covered entities that do not comply with the new NYDFS mandates may include fines, lawsuits, public exposure, loss of trust, and more. Potential "real world" scenarios for non-compliance might include revocation of licenses and fines of up to $250,000. Under banking laws within New York Consolidated Laws, penalties for violations can be as high as $25,000 per day.

Beyond NYDFS fines, Covered Entities are subject to New York State fines, breach disclosure consequences, and potential lawsuits for violating the state's General Business Laws and New York City Administrative Codes. Even prior to the implementation of the recent mandates, the NYDFS gained a reputation for heavy-handed enforcement. In 2016, the NYDFS collected billions of dollars in fines and settlements from dozens of leading financial institutions for compliance violations. New regulation guidelines under 23 NYCRR Part 500 will only increase the agency's reach and the severity of non-compliance.

NYDFS Best Practice Recommendations

To ensure full compliance, there are several best practices that Covered Entities should consider. Initially, IT and IS professionals should undertake a comprehensive security assessment to find the "holes" and identify areas of non-compliance or weakness. Below are some areas of focus under the new NYDFS mandates that should be reviewed to ensure compliance.

Overall program and policy framework

Covered Entities will need to establish and maintain an organization-wide cybersecurity program and policies that will enable them to comply by identifying, measuring, managing, and mitigating risks. The best practices recommendations to comply with these changes include reviewing your cybersecurity programs and creating and maintaining a document repository of your policies. You'll also want to evaluate your firm's nonpublic information (NPI) definition to validate that you're aligned with the NYDFS mandates. Most importantly, from an IAM perspective, understand clearly where your NPI is located and who has access to it. Be sure to limit this access to a "need to know and use" basis, and periodically review your user access privileges.

Risk assessment, testing, and compliance

Covered Entities should formally evaluate identity risks and the effectiveness of their access controls. All related systems and applications should be assessed and evaluated on a continuous basis—not just by the dates noted. The best practices recommendations to comply with these changes include improving your IAM visibility and ability to uncover access risks. Implementing effective MFA solutions can help by removing or restricting access for users that might pose risks or are under investigation. The best MFA solutions will prompt for extra verification and step-up authorization in the event of suspected unauthorized access.

Personnel, resources, and training

If your mission is to ensure compliance for a covered entity, you will need to employ a strong cybersecurity leader and verify they have the right people, resources, and organizational cybersecurity training. The best practices recommendations to comply with these changes include assessing your IAM policies and solutions, and having your CISO

implement effective IAM training. A key focus for this training should include educational elements related to password inadequacies, protecting credentials, and the sophisticated phishing and spearphishing techniques now employed by attackers.

Access, application security, and encryption

Covered Entities will need to effectively manage identity controls and application access and ensure you have properly encrypted NPI, or at least have an adequate plan in place to do so. The best practices recommendations to comply with these changes include a thorough review of your firm's IAM access privileges and authentication approaches, especially as related to application security, to validate that you're complying with the new mandates. Considerations here might include extending your IAM strategies to the cloud and mobile apps and ensuring proper access rights to all locations, as well as preventing insider threats and creating safeguards from account compromises. Reducing identity silos and attack surfaces and improving identity assurance is also key.

Finally, to ensure compliance with the NYDFS MFA guidelines, one of the first things a covered entity will want to review is its authentication technology. The four most common authentication types employed are: Single-Factor, Two-Factor (2FA), Multi-Factor, and Adaptive Multi-Factor. While each of these offer pluses and minuses, meeting NYDFS mandates requires MFA or an equivalent. Outlined below is the difference between MFA and Adaptive MFA.

Multi-Factor Authentication

MFA refers to methods that extend beyond Single-Factor or 2FA and offer the most robust IAM security. MFA transcends the black-and-white approach of either granting or denying access and offers a more effective type of authentication via a variety of methods. MFA uses multiple data points and factors derived from a login attempt, such as third-party hardware tokens, biometrics, or SMS.

The downside is that MFA can be disruptive if users must re-authenticate throughout their workday or use both hard and soft tokens to verify access. Adding authentication factors boosts security but may degrade the user experience. MFA systems can also be cumbersome for IT and IS teams that need to manage integrations with multiple applications or systems.

Adaptive Multi-Factor Authentication

The most innovative, effective, and non-disruptive form of authentication is Adaptive MFA. This advanced type of authentication matches system flexibility with how much risk a user presents. An Adaptive MFA service integrates a company's applications and resources to add a layer of authentication, and each time a user logs in, the system analyzes the request through backend analytics to determine how much access to grant.

For example, if an employee is working onsite and uses a security badge to enter the building, Adaptive MFA recognizes that the employee is in a trusted location and adjusts the level of identity access needed. If that same employee needs to gain access from an unsecure offsite location, the system may require additional authentication.

When reviewing which MFA solution to implement, Okta recommends examining three key best practice considerations:

Secure

Obviously, you'll want to review the capabilities of your MFA solution to ensure it meets all the standards and mandates required under the new regulations. Also, any solution implemented should help you avoid other security-related consequences such as lawsuits and fines while eliminating costly disruptions and user complaints. Three things to take into consideration here are:

- Full range of factor and assurance level support
- Adaptive functionality with step-up authentication for additional security without overburdening users
- Secure authentication for cloud, mobile, and on-premise applications

Simple

If you're moving away from a non-compliant 2FA solution, for example, you'll want to ensure that your new MFA solution offers ease-of-use and implementation via a non-disruptive, non-intrusive, easily integrated solution that works with your existing infrastructure like VPN and includes simple management and monitoring. Three things to consider here are:

- Usability and better overall experience for users
- Ease of management for administrators
- Flexible deployment options including phased deployments

Extensible

Okta recommends that any MFA solution considered be extensible for better productivity and quicker return on investment. Best practice solutions should include compatibility with third-party solutions and industry-proven reliability. Here are three additional things to consider:

- Out-of-the box integration with popular business applications
- Integration with custom apps with API support for unique use cases and needs
- Ability to work with existing security tools to extend security investments while providing meaningful authentication data

How Can Okta Help?

While it is important to note that Okta alone cannot ensure full NYDFS compliance, Okta's IAM solutions can certainly fulfill the access and authentication requirements specified while also providing a strong security foundation.

MFA is mandated under the new NYDFS guidelines in Section 500.12, and Okta's Adaptive MFA solution can meet all requirements for compliance. Okta Adaptive MFA ensures security across virtually any application, whether in the cloud, on personal mobile devices, or on premise, and for all user groups. With a full range of factors across the entire assurance spectrum, Okta Adaptive MFA reduces security risks by hardening access based on dynamic device and user context. Compliance is assured with a solution that is easy to use, deploy and manage. With over 5,000 out-of-the-box connections on the Okta Integration Network and API support for custom applications, Okta Adaptive MFA extends across the entire organization. Okta connects business applications and ensures seamless productivity and integration with a variety of security tools for end-to-end visibility and improved security.

The new NYDFS mandates specify that access controls must be "based on the individual facts and circumstances presented." As such, your access controls must be underscored by realistic and clearly defined cybersecurity policies that consider user identities, roles within your firm (or outside in the case of third-parties), and which specific

areas, information, and apps certain individuals should be allowed to access. Along with Okta's Adaptive MFA, Okta's sophisticated Lifecycle Management ensures orchestration and entitlement management to maintain the optimal level of access to your applications. You can easily set access and entitlement rules based on attributes, such as user group membership. You can also provide visibility into who has access to what data through simple access governance, gain visibility into all users who have access to specific applications, and much more.

The challenge for most IT and IS professionals will be in balancing your firm's ability to comply against the possibility of injecting undue obstacles that might hinder user productivity. The table below describes specific NYDFS regulation requirements on the left and relates them to Okta solutions on the right that can help ensure compliance without causing unwanted disruptions.

	Regulation Requirement	How Okta Can Help
500.02	Cybersecurity program, (b)(1)–Covered Entities must identify and assess internal/external cybersecurity risks	• Okta's syslog/reporting can provide centralized views into all authentication data across cloud, mobile, and on-premise applications. • Anomalous events are surfaced in the syslog and include brute force detections, anomalous login/location/client detections, low reputation network login detections, and more.
500.03	Cybersecurity policy, (d)–a Covered Entity's policies must cover access controls and identity management	• Okta's identity-led security framework can solve IAM control challenges by centralizing identity, enforcing strong authentication everywhere, reducing attack surfaces with automated provisioning/deprovisioning, and by enabling visibility and response.

500.06	Audit trail, (a)(1) - logging, (a)(2)–a Covered Entity's audit trails must be designed to detect and respond to cybersecurity risk events	• Okta's syslog/reporting can offer a centralized view into all authentication data across cloud, mobile, and on-premise applications. • Anomalous events are surfaced in the syslog and include brute force detections, anomalous login/location/client detections, low reputation network login detections, and more. • Admins can take action based on detected events, such as prompting for step-up authentication, limiting or revoking access, changing user group membership, and more.
500.07	Access privileges–Covered Entities must limit user access privileges to non-public info and review those privileges periodically	• Sophisticated lifecycle orchestration and entitlement management can ensure the right level of access to the right applications. • You can easily set access and entitlement rules based on attributes, such as user group membership. • Okta provides visibility into who has access to which data via simple access governance that offers the ability to see all users who have access to specific applications.
500.09	Risk assessment, (a)–Covered Entities must conduct periodic risk assessments	• Okta's syslog/reporting can offer a centralized view into all authentication data across cloud, mobile, and on-premise applications. • Anomalous events are surfaced in the syslog and include brute force detections, anomalous login/location/client detections, low reputation network login detections, and more.

500.12	MFA, (a) Covered Entities must use MFA/risk-based authorization, (b) Covered Entities must use MFA for external-to-internal resource access	• Okta Adaptive MFA affords intelligent, contextual access based on user and device attributes. • Okta's flexible policy framework allows for step-up authentication based on risk-based user or device context such as anomalous location, brute force attempts, etc. • Okta's flexible and granular policy framework allows different MFA policies for different user types including admins, users, and third parties (contractors and partners, etc.). • Okta's multiple network zone support allows policies to be defined for access from outside your firm's network.
500.14	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	• Okta's syslog/reporting can offer a centralized view into all authentication data across cloud, mobile and on-premises applications. • Anomalous events are surfaced in the syslog and include brute force detections, anomalous login/location/client detections, low reputation network login detections, and more. • Okta's flexible policy framework allows for step-up authentication based on risk-based user or device context such as anomalous location, brute force attempts, etc.

Conclusions

The new NYDFS regulation affects a wide range of Covered Entities within or related to the financial industry and which operate or do business in the State of New York. These mandates specify that Covered Entities must complete a cybersecurity program risk assessment to determine if current best practices and policies will adequately mitigate risks related to exposure or loss of NPI and other sensitive information.

IAM is a key ingredient in providing a front line of defense and to ensure compliance, and the NYDFS specifically calls out MFA or its equivalent as a requirement. Covered entities must prove they have adequate IAM systems in place that eliminate or mitigate the ability of hackers, phishers, insiders, or third parties to have unauthorized access to sensitive information. The NYDFS has outlined specific dates to ensure all proper measures and policies are in place.

IT and IS professionals and executives involved with security must now view IAM, and especially MFA, as a vital component to protect sensitive and valuable information from exposure or theft, and to comply with the regulations.