NYCRR (NYDFS) Compliance

Beyond Identity

BEYOND IDENTITY

Overview

In 2017, New York Department of Financial Services (NYDFS) issued a cybersecurity regulation (23 NYCRR Part 500) that all financial services companies that service New York residents, including those registered outside of New York state, are subjected to.

A critical component of this regulation is the implementation of multi-factor authentication (MFA) or risk-based authentication. In fact, NYDFS issued follow up guidance calling out that "MFA weaknesses are the most common cybersecurity gap exploited at financial services companies. Since the Cybersecurity Regulation went into effect, DFS has scrutinized hundreds of cyber incidents at DFS-licensed organizations ("Covered Entities"), and seen MFA gaps exploited over and over again."

Beyond Identity helps you meet and exceed the MFA and risk-based authentication requirements as mandated by NYDFS.

Who does NYDFS apply to?

This regulation applies to "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."

This means organizations registered outside of New York state that service New York residents must comply with NYDFS requirements.

Some examples of the types of companies that are considered a covered entity under this regulation include but are not limited to:

Banks	Trust companies
Investment companies	Mortgage bankers
Licensed lenders	Holding companies
Budget planners	Health insurers
Life insurance companies	Charitable foundations

Exemptions are very limited and covered entities are broad. The only exemptions are for organizations with fewer than 10 employees (including contractors), less than $5M in gross revenue from New York business operations, and less than $10 million in year-end total assets.

What's the impact of NYDFS?

Fines:

- DFS Investigation Uncovers National Securities Corporation Failed to Implement Multi-Factor Authentication, Falling Victim to Four Cyber Breaches that Exposed its Customers' Private Data - *$3M fine*
- First Unum and Paul Revere Life Insurance Failed to Implement Multi-Factor Authentication, Falling Victim to Two Phishing Attacks that Exposed Consumers' Personal and Private Data - *$1.8M fine*

Actively reviewing MFA compliance:

- From January 2020 to July 2021, DFS found that more than 18.3 million consumers were impacted by cyber incidents reported to DFS had MFA failures…DFS is also increasing its review of MFA during examinations, with a particular emphasis on probing for the common MFA failures (weak MFA, incomplete rollout, lack of coverage for cloud-based applications, etc.).

Lowered customer satisfaction scores:

- Authentication friction causes the satisfaction scores to decrease and drop-off to competitors.

NYDFS Multi-Factor Authentication, Risk-Based Authentication & Beyond Identity

A key component of NYDFS regulation is the implementation of MFA or risk-based authentication.

Further emphasizing the criticality of MFA, following the release 23 NYCRR Part 500 in 2017, NYDFS issued an industry letter in December 2021 stating that "MFA weaknesses are the most common cybersecurity gap exploited at financial service companies" and provided an overview of common MFA challenges organizations need to overcome.

This table correlates the NYDFS requirements and its subsequent industry letter with Beyond Identity's capabilities to meet and exceed those requirements.

	Requirement Details	*Beyond Identity*	*Differentiation*
NYCRR Part 500	500.12(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.	✓	Unphishable MFA with: • Something you have - possession of private key within device secure enclave • Something you are - local device biometric Every authentication is evaluated for real-time device risk at time of authentication and continuously.
	500.12(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.	✓	Every authentication with Beyond Identity is multi-factor by default. Given our architecture, each device is cryptographically bound to a specific user identity to ensure that the right person, with a secure device, is accessing the right data.
NYDFS Industry Letter	Oversight in deprecating legacy systems that don't support MFA (such as Microsoft email services).	✓	Beyond Identity integrates with all major modern IDPs/ IDaaS solutions as part of our strong authentication transformation.
	MFA for remote access fails to cover key applications since cloud-based services are able to be accessed without VPN access (such as O365 or G-Suite).	✓	Beyond Identity closes the blind spot over cloud-based services by verifying device trust across all endpoints (managed and unmanaged) and enforcing compliance with your adaptive access policies.
	Lack of MFA for third parties that have access to an internal network with nonpublic information.	✓	Beyond Identity lowers MFA friction to zero and makes it more easily adopted by all applications and users including third parties.
	MFA setups and rollouts that are not completed for all users in a timely manner. When left to the user to set up, some users never set up MFA.	✓	Beyond Identity removes the burden of MFA adoption from the users by delivering unphishable MFA by default that is invisible to the users. Given our broad support for open standards, integration and rollout is fast and easy.

NYDFS Industry Letter	Poor exceptions management whereby the organization provided too many exceptions to MFA policy or allowed permanent exceptions (such as "C-Suite exemption).	✓	Beyond Identity's policy engine centralizes authorization decisions and reduces the desirability of one-off exclusions. Additionally, with zero-friction invisible MFA, adoption is painless for end-users.
	MFA should be used for all privileged accounts.	✓	Beyond Identity's zero-friction, invisible MFA allows for consistent and strong authentication of all users across all applications.
	Not all MFA are equal: Push-based MFA is more susceptible to human error than token-based MFA and text-based MFA is vulnerable to SIM-swapping.	✓	Our architecture is designed to deliver MFA that only uses unphishable factors and does not rely on shared secrets, push notifications, tex-based codes, nor magic links.
	Oversight of MFA: test and validate effectiveness of MFA via audits, pentests, and vulnerability scans.	✓	Beyond Identity provides an admin console with immutable event logs for all transactions that can be exported or forwarded to any SIEM. This includes the security posture of the device at the exact time of authentication, successful and failed authentications along with the reason for the outcome, device changes, policy changes, and more to simplify compliance audits and reporting.

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.