NY DFS Multi-Factor Authentication Requirements

In 2023, the New York State Department of Financial Services (DFS) amended its landmark cybersecurity regulation 23 NYCRR Part 500 with new requirements starting in Nov 2023 and going through Nov 2025.

Included in the regulation's amendment are updates to Section 500.12, which requires Covered Entities from the Small Business, Standard, and Class A categories to comply with enhanced multi-factor authentication (MFA) requirements. With limited exceptions, Covered Entities must implement MFA for any individual accessing any of its information systems. This document provides information on MFA and the regulation's requirements.

What is MFA?

MFA is a key security control that provides an enhanced means of verifying the identity of a user by requiring a user to provide at least two of three types of authentication factors at login. Each factor adds a distinct layer of protection, significantly reducing the risk of unauthorized access. The categories of factors are:

Something you know, such as a password, passphrase, or personal identification number (PIN)

Something you have, such as a hardware token, authentication app, or smartcard

Something you are, such as fingerprints, facial recognition, or other biometric markers

Why is MFA Necessary for Financial Services Institutions?

MFA adds a critical layer of protection by requiring at least two forms of verification, making it much harder for threat actors to gain unauthorized access to information systems, even if a password is compromised. This is especially important in the financial sector, where credential-based attacks are common. MFA helps prevent account takeovers, data breaches, and other high-impact cyber incidents.

Variation in MFA Methods

While all MFA methods aim to add an extra layer of protection, their effectiveness can vary significantly based on how they are deployed and the specific threats they are designed to defend against. It is important for organizations to understand the trade-offs associated with each method in order to make informed, risk-based decisions.

Some examples of MFA methods are:

- **SMS Authentication,** which requires users to enter a digital code or token that has been sent to their cell phone via SMS text message. This method is widely available but generally considered a weaker authentication method as it is susceptible to SIM-swapping and interception.

- **App-based Authentication (no number matching),** which requires users to download a pre-authorized, MFA-compliant application onto their phone that will receive a push notification asking for permission to gain access to a network. This method is convenient but vulnerable to push fatigue attacks.

- **App-based Authentication (with number matching),** which requires users to download a pre-authorized, MFA-compliant app onto their phone that asks users to enter a digital code or token before gaining access. This method is more secure and helps to prevent unauthorized approvals.

- **Token-based Authentication,** which requires a user to maintain physical possession of a hardware token that prompts a user to authenticate attempts to login to an account or otherwise verify an action within an information system. This method provides strong protection through physical possession, though its availability is more limited and, as a result, deployment can be more complex.

When are Covered Entities Required to Implement MFA?

Covered Entities are currently required to utilize MFA for individuals accessing their internal networks from an external network, unless its Chief Information Security Officer (CISO) approves, in writing, alternative controls. Starting on November 1, 2025, Covered Entities will be required to use MFA for any individual accessing any of its information systems, regardless of location, type of user, and type of electronic information contained on the information system being accessed, among other things. There are two exceptions:

1. The Covered Entity has a CISO that approves in writing the use of reasonably equivalent or more secure compensating controls (and reviews this determination periodically but at a minimum annually), or
2. The Covered Entity qualifies for a limited exemption pursuant to Section 500.19(a). In this case, MFA is only required for:

    - Remote access to the covered entity's information systems;

    - Remote access to third-party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and

    - All privileged accounts other than service accounts that prohibit interactive login.

For more information about the MFA requirements and DFS's Cybersecurity Regulation, including FAQs, timelines, videos, and other resources, visit the Department's Cybersecurity Resource Center.