Department of Financial Services

# Industry Guidance

**Re: Guidance on Multi-Factor Authentication**

**Introduction**

Multi-Factor Authentication ("MFA") is an essential part of cybersecurity hygiene. This was true even in 2016 and 2017, when the Department of Financial Services ("the Department" or "DFS") drafted 23 NYCRR Part 500 (the "Cybersecurity Regulation" or the "Regulation"). MFA was already considered an essential control, which is why it was one of the few technical controls explicitly required by the Regulation.[1] MFA's importance hasn't changed – if anything, the increase in cybercrime has made MFA even more essential.

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"),[2] and seen MFA gaps exploited over and over again. The most common weaknesses are described below and include MFA being absent, not fully implemented, or configured improperly.

MFA failures have real consequences for financial services companies and consumers. In fact, from January 2020 to July 2021, DFS found that more than 18.3 million consumers were impacted by cyber incidents reported to DFS pursuant to Section 500.17(a) ("Cybersecurity Events")[3] in which Covered Entities had MFA failures. Over 870 thousand of those consumers were New Yorkers.

MFA is therefore a focus of DFS's cybersecurity supervisory and enforcement work. As part of this focus, DFS has resolved two enforcement actions in the past year against companies that were required to implement MFA but had not fully done so and that failed to prevent unauthorized access to their nonpublic information.[4] DFS is also increasing its review of MFA during examinations, with a particular emphasis on probing for the common MFA failures discussed in this Guidance.

Growing cyber risk and the importance of MFA should be carefully considered by Covered Entities as they implement the risk-based cybersecurity program required by the Cybersecurity Regulation. Cybercrime and cyber risk have grown steadily over the past two decades, and that growth accelerated during the pandemic as a result of the extraordinary number of people who started working remotely.[5] The Cybersecurity Regulation requires MFA for remote access, and for MFA to be implemented beyond that as necessary to ensure effective access controls based on a comprehensive risk assessment.[6] Given the high and growing level of risk posed by a lack of MFA, Covered Entities should ensure that MFA is implemented effectively and that MFA is used wherever it is needed to manage the risk of unauthorized access.

MFA is important for all businesses, whether large or small. While many small businesses licensed by DFS are exempt from the requirement to use MFA for remote access, unfortunately they are not exempt from being targeted by cybercriminals. The increase in cybercrime has hit small businesses hard, and DFS has reviewed many incidents at small businesses where cybercriminals exploited the fact that MFA was not implemented.[7] In the wake of such attacks, the great majority of these small

businesses decided to implement MFA as part of their remediations. The reputational and financial damage, however, was already done.

The Department is committed to protecting consumers and securing the safety and soundness of DFS-regulated organizations. Effective implementation of the Regulation's MFA requirement is one of the most potent ways to reduce cyber risk.

**I. Common Problems Related to MFA and Recommendations**

Lack of effective MFA has been the most frequently exploited cybersecurity gap in the Cybersecurity Events reported to the Department. Approximately 64% of Covered Entities that reported Cybersecurity Events from January 2020 to July 2021 had some gap in their MFA. In some cases MFA was completely absent; in others it was not enabled, misconfigured, only partially implemented, or pending implementation.

The Cybersecurity Regulation contains several requirements relating to MFA. In general, all Covered Entities are required to implement risk-based cybersecurity programs and policies that, among other things, adopt appropriate protections from unauthorized access.[8] More specifically, Covered Entities that have not filed a Notice of Exemption pursuant to Section 500.19 must use MFA for remote access to all internal networks, including applications and systems, unless their CISOs have approved "the use of reasonably equivalent or more secure access controls."[9]

**A. Violations of DFS's Cybersecurity Regulation**

Too many cyber incidents reported to DFS involve violations of the Section 500.12 requirement for MFA. The following are the most common reasons for such violations.

**1. Legacy Systems That Do Not Support MFA**

Gaps in MFA coverage arise when Covered Entities use outmoded applications and systems ("legacy systems") that do not support MFA. The most commonly exploited legacy system is Microsoft email services which employ only basic, non-MFA legacy authentication. Microsoft announced that it is disabling basic authentication in favor of modern authentication, but the transition has been delayed due to the pandemic. Covered Entities should elect modern authentication over basic authentication when using Microsoft's email services.

In several reported cyber incidents, an attacker exploited a legacy system that the Covered Entity did not realize was still active. The Covered Entities migrated to a modern system, implemented MFA, but simply forgot about, or missed disabling, the unneeded legacy systems. To prevent such oversights, Covered Entities must maintain an up-to-date inventory of all IT assets and regularly decommission systems that are no longer needed.

**2. MFA for Remote Access Fails to Cover Key Applications**

While most VPN services require the use of MFA, many Covered Entities have email or other applications that can be accessed without VPN access. The Department has seen many incidents that occurred because MFA was not in place for remote access to a core function like email. A common problem is a lack of MFA for cloud-based services such as O365 or G-Suite. Covered Entities must therefore ensure that MFA is in place for remote access to all applications and systems, including those that can be accessed without authenticating through a VPN.[10]

**3. Lack of MFA for Third Parties That Have Access to an Internal Network with Nonpublic Information**

Covered Entities sometimes do not require third parties to use MFA when accessing their systems and the nonpublic information on them. For example, insurance companies sometimes do not require MFA for independent insurance agents who have access to sensitive consumer information – such as social security numbers and drivers' license numbers – on the insurance companies' information systems. The Department has seen a number of cyber incidents targeting these third-party portals and applications through phishing and credential stuffing.[11] To prevent this type of unauthorized access, Covered Entities must require MFA or the use of reasonably equivalent or more secure access controls for all third parties accessing information systems with nonpublic information.

**4. MFA Setups and Rollouts That Are Not Completed for All Users In a Timely Manner**

An MFA setup or rollout that is incomplete or slow can leave gaps in MFA coverage. Granting remote access permissions and configuring MFA for users should be done with the direct oversight of one or more designated individuals. The Department has seen several cyber incidents that occurred when attackers exploited MFA "self-setup" to setup MFA controlled by the cybercriminal. Additionally, the Department has seen cyber incidents that occurred because MFA setup was left to the user, and some users never setup MFA. Covered Entities should track and enforce compliance with the MFA requirement.

The Department has also reviewed incidents that occurred because of long gaps in MFA coverage during rollouts or transitions to new technology. In some cases these gaps lasted for many weeks or months. Covered entities should plan transitions to avoid gaps in MFA usage and implement compensating controls during temporary gaps.

**5. Poor Exceptions Management**

The Department has reviewed cyber incidents that occurred because a Covered Entity granted too many exceptions to MFA policy or allowed permanent exceptions. These problems with exceptions often occurred because of a lack of a clear policy on exceptions, failure to enforce policies such as time limits on exceptions, and/or failure to track exceptions. Exceptions to the MFA requirement should be granted sparingly, tracked, and last only as long as necessary.

The Department has reviewed several Cybersecurity Events resulting from the so-called "C-Suite exemption," where a senior member of the company simply refused to use MFA. Exceptions should not be granted based on the seniority or unwillingness of the user.

**B. Other Considerations**

Covered entities should be considering MFA as a key component of all access controls, especially in light of the growing risk of cyber incidents that exploit MFA weaknesses. When implementing risk-based access controls as required by Sections 500.3 and 500.12(a), Covered Entities should therefore think about the following.

**1. MFA for Privileged Accounts**

In every case where cybercriminals escalated privileges during a reported Cybersecurity Event, the privileged account lacked MFA. Privileged accounts should be carefully protected to prevent cyber criminals from escalating privileges as doing so is necessary for successful ransomware and other cyberattacks. Given the risk here, Covered Entities should use MFA for all privileged accounts, as discussed in our Ransomware Guidance[12] and by the Cybersecurity & Infrastructure Security Agency ("CISA") and the Federal Bureau of Investigation in their warning to remain vigilant against malicious cyber actors.[13]

**2. Not all Forms of MFA are Equal**

The most common types of MFA used by Covered Entities are token-based or push-based configurations. Token-based MFA requires a user to manually enter a one-time use passcode generated by a hardware or software device. In contrast, push-based MFA only requires a user to accept an on-screen prompt or press a button in response to an automated phone call. Push-based MFA is more susceptible to human error than token-based MFA. DFS has seen several Cybersecurity Events where inattentive users allowed a cybercriminal to gain access to the user's account by authenticating push-based MFA. With token-based authentication, a user is less likely to unwittingly grant access to a cybercriminal because the user must proactively enter a passcode.

Text message-based MFA is vulnerable to SIM-swapping. SIM swapping occurs when a scammer steals a victim's phone number by switching the phone number from the victim's device to a device controlled by the scammer. SIM-swapping allows the scammer to then steal any MFA codes sent to the victim's phone number.[14]

**3. Oversight of MFA**

Covered Entities should also test and validate the effectiveness of MFA implementation. IT audits, penetration tests, and vulnerability scans should include verification of MFA control strength and identification of weaknesses or gaps

in MFA as implemented and configured. Material weaknesses must be reported to the Board.

**II. Small Businesses and MFA**

Small businesses find themselves increasingly in the crosshairs of cyber criminals eager to exploit a lack of MFA. As the U.S. Small Business Administration has noted, small businesses are being aggressively targeted because "they have information cybercriminals want, and they typically lack the security infrastructure of larger businesses."[15] Last year, 23% of small businesses suffered cyberattacks and many small businesses incurred losses in the hundreds of thousands of dollars.[16] Immediate costs include restoring systems, forensic analysis, legal bills, downtime, and more.[17] Further, the reputational harm with customers and increased cyber insurance premiums are particularly difficult for small businesses to absorb.[18]

As with larger companies, a lack of MFA is the leading cybersecurity gap exploited in attacks against small businesses regulated by DFS. Of those small businesses that reported Cybersecurity Events to DFS between January 2020 and June 2021, approximately 82% had deficiencies with respect to MFA. As part of their remediation plans post-attack, almost all of these entities decided to implement MFA because it is one of the most cost-effective ways to reduce the risk of a cyber incident – according to one recent survey, the cost is only $33 per employee.[19]

The Department therefore recommends that small businesses implement MFA. DFS recognizes that cybersecurity can be especially challenging for small businesses, and has worked to make cybersecurity easier by partnering with the Global Cyber Alliance ("GCA") to bring GCA's Cybersecurity Toolkit for Small Business to financial services companies.[20] The Toolkit includes practical tools and instructions for implementing the essentials of cybersecurity hygiene. This includes step-by-step instructions for implementing MFA in applications often used by small businesses, such as Google and Microsoft products. We urge small business to take advantage of the GCA's Toolkit and other resources, such as CISA's Cybersecurity Awareness Program Small Business Resources.

---

[1] See 23 NYCRR § 500.12.

[2] See 23 NYCRR § 500.1(c) (defining "covered entity" for purposes of the Cybersecurity Regulation).

[3] See 23 NYCRR § 500.1(d) (defining "cybersecurity event" for purposes of the Cybersecurity Regulation).

[4] See In the Matter of National Securities Corporation; In the Matter of First Unum Life Insurance Company and the Paul Revere Life Insurance Company.

[5] See DFS's Guidance Regarding Cybersecurity Awareness During Covid-19 Pandemic dated April 13, 2020; Signal, September 1, 2021, 81 Ransomware Statistics, Data, Trends and Facts for 2021 ("Due to the rise in remote work prompted by the pandemic, [ransomware] attacks are up 148%.").

[6] See 23 NYCRR § 500.12.

[7] All entities should consider whether to implement MFA in their risk assessments even if they are exempt from the MFA requirements under 23 NYCRR § 500.19(a).

[8] See 23 NYCRR §§ 500.2 and 500.3(d).

[9] 23 NYCRR § 500.12(b).

[10] See 23 NYCRR § 500.12(b) (MFA is required when accessing internal networks from external networks); FAQ 40, Cybersecurity Resource Center (Internal networks include a Covered Entity's email system, whether based in the cloud or on premises.).

[11] See, e.g., DFS's Cyber Fraud Alert dated February 16, 2021 and DFS's Cyber Fraud Alert Follow-Up dated March 30, 2021.

[12] See DFS's Guidance on Ransomware Prevention dated June 30, 2021. Moreover, pursuant to Section 500.12(a), Covered Entities must consider in their risk assessments whether they should require MFA for privileged accounts.

[13] See CISA, Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends, released November 22, 2021 (urging organizations to implement MFA "for remote access and administrative accounts" in order to protect themselves "from becoming the next victim").

[14] See T-Mobile Data Breach and SIM-swap Scam: How to Protect Your Identity.

[15] U.S. Small Business Administration, Stay Safe from Cybersecurity Threats.

[16] See Hiscox Cyber Readiness Report 2021 at 9.

[17] See Allianz, Cyber Insights Ransomware Trends: Risks and Resilience (October 2021) at 7; Verizon, 2021 Data Breach Investigations Report at 26.

[18] See Hiscox Cyber Readiness Report 2021 at 9.

[19] See Bio-Key, The State of MFA at 12. Additionally, MFA it is now a standard feature in almost all commercial software products. For example, in Microsoft Office 365, MFA protection is included in the software package as a default setting. See Microsoft, Turn on Multi-factor Authentication (accessed July 6, 2021).

[20] See DFS, Information for Small Businesses, Cybersecurity Tools.