FIDO Alliance Input to the New York Department of Financial Services (DFS)

Proposed Cybersecurity Requirements for Financial Services Companies – 23 NYCRR Part 500

January 2023

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to provide comments to the New York Department of Financial Services (DFS) on its proposed Cybersecurity Requirements for Financial Services Companies – Second Amendment to 23 NYCRR 500.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 300 companies and government agencies from around the world dedicated to the creation of standards and certification programs for Multi-Factor Authentication (MFA) and passwordless authentication, as well as remote identity verification.

Our 40+ board members, whose logos are included below, demonstrate the strength of the FIDO Alliance's leadership, as well as the diversity of its membership. Our members include leading firms in banking, payments, telecommunications, and fintech, as well as those in security, health care, and information technology.

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eight years that have followed – has helped to transform the authentication market, addressing concerns about the problems with passwords, as well as the increasing phishability of legacy, first-generation MFA tools like One Time Passwords (OTPs) while also enabling significant improvements in the usability of MFA.

Today, the FIDO2 standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication that is both more secure and also easier to use than legacy MFA tools.

As the White House's recent Federal Zero Trust Strategy notes, FIDO2's Web Authentication standard *"is supported today by nearly every major consumer device and an increasing number of popular cloud services."*[1] Apple, Google, and Microsoft have all embedded support for FIDO2 at the device, operating system, and browser level, enabling new models for deployment phishing-resistant MFA to be "built in" rather than "bolted on."

The increasing ubiquity of FIDO support in commercially available smartphones, laptops and other computing devices has created new options for consumer authentication that improve security, privacy, and usability.

[1] https://zerotrust.cyber.gov/federal-zero-trust-strategy/

As DFS considers new regulations here, we offer three comments:

1. **DFS should consider strengthening its language on authentication to call for phishing-resistant authentication – in line with recent guidance from the White House, Cybersecurity and Infrastructure Security Agency (CISA), and the Consumer Financial Protection Bureau (CFPB).**

   We raised this point in an earlier round of comments to DFS submitted in August 2022, and were surprised to see this issue was not addressed in the latest draft. As written, the current proposed language conflicts with language on MFA from DFS's 2020 Twitter report, as well as recent guidance from both CFPB and CISA at the Federal level – providing somewhat confusing guidance to financial institutions.

   Given how attacks against legacy MFA have continued to grow more sophisticated, DFS should go farther – and specifically call for the use of phishing-resistant authentication, in line with recent guidance from the White House, CISA, and CFPB.

   In recent years, criminals have found ways to easily compromises some other forms of MFA through phishing attacks, including one-time password (OTP) apps and those authenticators which ask users to approve a login through a push notification. As the White House's recent Zero Trust Strategy[2] noted:

   > *"Many approaches to multi-factor authentication will not protect against sophisticated phishing attacks, which can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale."*

   This point was also made by DFS in its 2020 Twitter Investigation Report, where DFS flagged the problems with using app-based MFA, and guided implementers to using physical security keys (such as FIDO Security Keys) that cannot be phished or easily compromised.[3] Per that report:

   > *"MFA is critical, but not all MFA methods are created equal. Twitter used application-based MFA, which sent a request for authentication to an employee's smart phone. This is a common form of MFA, but it can be circumvented. During the Twitter Hack, the Hackers got past MFA by convincing the Twitter employees to authenticate the application-based MFA during the login. The most secure form of MFA is a physical security key, or hardware MFA, involving a USB key that is plugged into a computer to authenticate users. This type of hardware MFA would have stopped the Hackers, and Twitter is now implementing it in place of application-based MFA."*

   Both DFS and the White House flagged an important point, which is that as criminals continue to evolve their attack methods, it is important that regulators update their regulations to reflect the current attack landscape. Today the risk is not just that SMS-based authenticators are compromised but that any authenticator based on shared secrets can be compromised through phishing attacks, including OTP and push-based authentication tools.

   We note that DFS seemed to backtrack from its guidance in the Twitter report with regard to Security Keys in its December 2021 updated guidance on MFA,[4] making no mention of Security Keys at all, and suggesting that that having to proactively enter a one-time passcode (OTP) somehow protects against the kinds of attacks that might compromise push-based solutions.

[2] https://zerotrust.cyber.gov/federal-zero-trust-strategy/#identity

[3] https://www.dfs.ny.gov/Twitter_Report

[4] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance

Per the December 2021 publication:

> ***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.*

We note:

1) This December 2021 language conflicts with the language from the 2020 Twitter report – providing somewhat confusing guidance to financial institutions.
2) Relying on one-time passcodes (OTP) that have to be manually entered will not prevent those codes from being phished. Motherboard had a very good article on this point in November 2021 detailing how automated bots are now being used to steal OTP codes tied to financial services.[5]

To address this conflict – and ensure that financial institutions are protected against phishing attacks that compromise legacy MFA – DFS should strengthen its language on MFA to call for use of phishing-resistant authentication, in line with recent guidance from the White House, CISA, and CFPB.

As noted above, the White House Zero Trust Strategy flagged the ways that legacy MFA is being compromised and stated: *"For agency staff, contractors, and partners, phishing-resistant MFA is required."*

Per the White House Zero Trust Strategy:

> *"Fortunately, there are phishing-resistant approaches to MFA that can defend against these attacks…the World Wide Web Consortium (W3C)'s open "Web Authentication" standard, another effective approach, is supported today by nearly every major consumer device and an increasing number of popular cloud services.*
>
> *"Web Authentication, also known as WebAuthn, was developed as part of the FIDO Alliance's FIDO2 standards, and is now published by the World Wide Web Consortium (W3C) as a free and open standard.*
>
> *"Public-facing agency systems that support MFA must give users the option of using phishing-resistant authentication. Because most of the general public will not have a PIV or CAC card, agencies will have to meet this requirement by providing support for Web Authentication-based approaches, such as security keys."*

DFS should adjust the language in its MFA section to align with the White House's recent guidance.

Note that the White House is not the only government entity to flag concerns about phishing and recommend the FIDO2 and Web Authentication standard. CISA also updated its guidance on MFA[6] earlier this year, stating:

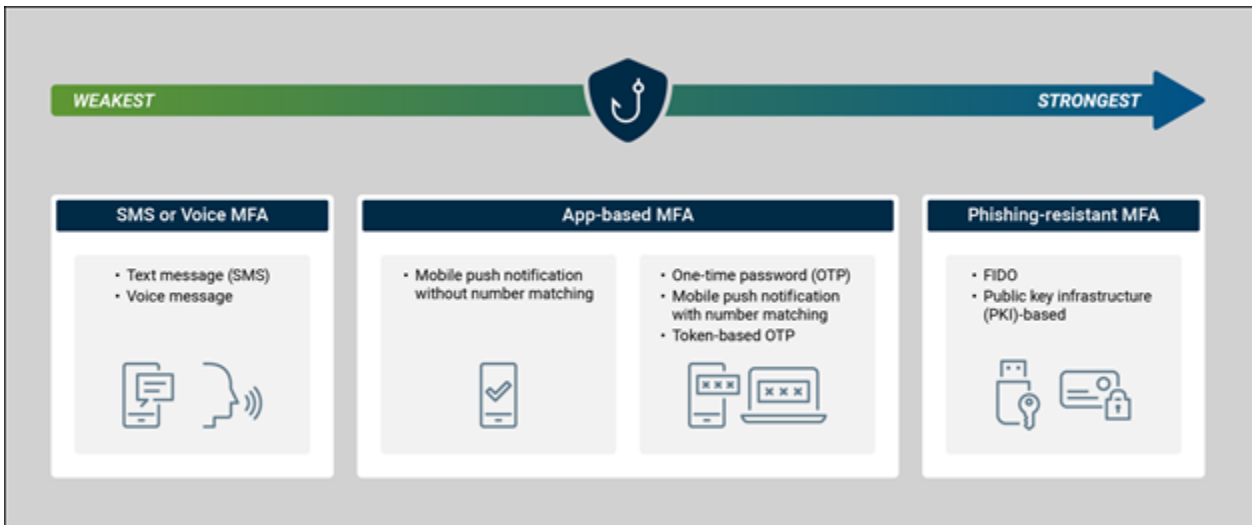
[5] See "The Booming Underground Market for Bots That Steal Your 2FA Codes" https://www.vice.com/en/article/y3vz5k/booming-underground-market-bots-2fa-otp-paypal-amazon-bank-apple-venmo

[6] https://www.cisa.gov/mfa

"Not all MFA methods gives you the same level of protection. Some MFA types are better than others—phishing-resistant MFA is the standard all industry leaders should strive for, but any MFA is better than no MFA. You should still strive to implement stronger MFA to avoid being hacked.

- *The only widely available phishing-resistant authentication is FIDO/WebAuthn authentication. CISA urges all organizations to start planning a move to FIDO because when a malicious cyber actor tricks a user into logging into a fake website, the FIDO protocol will block the attempt. See CISA Fact Sheet Implementing Phishing-Resistant MFA, CISAJen's blogpost Next Level MFA: FIDO authentication, and the Fido Alliance's How Fido Works for more information.*
- *If you can't currently implement phishing-resistant MFA, consider using numbers matching MFA to block mobile push bombardment and SMS-based attacks. See CISA Fact Sheet Implementing Number Matching in MFA Applications for more information."*

CISA also created a graphic depicting their "MFA Hierarchy" to help guide implementers as they make choices on what types of MFA to implement.



CFPB has followed CISA here. An August 11, 2022 circular from the CFPB[7] flagged the importance of phishing-resistant authentication to financial institutions, noting in new guidance on MFA:

"MFA solutions that protect against credential phishing, such as those using the (FIDO) Web Authentication standard supported by web browsers, are especially important."

Likewise, the National Institute of Standards and Technology (NIST) has stated that its upcoming refresh of its Digital Identity Guidelines (SP 800-63) will include language to differentiate phishing-resistance authentication from legacy MFA tools that are susceptible to phishing.[8]

At a minimum, we believe DFS should ensure that phishing-resistant MFA is used for privileged accounts, given the emphasis that the proposed changes to Section 500.12 give to protecting these accounts.

Short of a mandate, it also may be helpful in terms of "nudging" implementers to state that "In the event a covered entity suffers an intrusion, the Department will view favorably those entities that have widely deployed phishing-resistant MFA."

[7] https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

[8] See https://github.com/usnistgov/800-63-4/issues/3

2. **We were pleased to see DFS call for the wider use of MFA for remote access and privileged accounts.**

   There is no such thing as a "secure" password these days. A key flaw of passwords is that shared secrets rarely stay secret. The website haveibeenpwned.com tracks accounts that have been compromised in a data breach. At present, there are more than 11.89 Billion "pwned" accounts representing more than 847 Million real world passwords exposed in data breaches.[9] It is a security imperative for the country to reduce the use of passwords alone for authentication and shift businesses and consumers to multi-factor and/or passwordless authentication.

3. **We were pleased to see DFS propose to strike text messages as an allowable "possession factor" in MFA.**

   SMS was never designed to be used for authentication, and NIST advised organizations to stop using SMS for authentication in 2016. However, many organizations continue to rely on SMS as a second factor because it is cheap and easy to deploy; with its use, criminals have continued to ramp up attacks against SMS-based authentication, particularly phishing attacks that look to trick victims into handing over the one-time passcodes that are sent to them via SMS.

   Now that attackers have caught up with SMS tools used in authentication, the time is right to guide industry to the use of stronger, more resilient authentication tools.

We greatly appreciate DFS' consideration of our comments. We look forward to further discussion with DFS on this topic and would welcome the opportunity to answer any questions or collaborate on approaches to address some of the issues we raised in this response. Additionally, we are available to present an overview of FIDO standards and the FIDO Alliance, should DFS staff officials desire to learn more about how FIDO authentication and how its certification programs work.

Please contact our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our government engagement advisor, Jeremy Grant, at jeremy.grant@venable.com.

[9] Per https://haveibeenpwned.com/