fido ALLIANCE | simpler stronger authentication

FIDO Alliance Input to the SEC

Proposed Cybersecurity Risk Management Rules for Investment Advisers, Registered Investment Companies, and Business Development Companies

April 2022

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to provide comments to the Securities and Exchange Commission (SEC) on its Proposed Cybersecurity Risk Management Rules for Investment Advisers, Registered Investment Companies, and Business Development Companies - File Number S7-04-22.

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 the SEC considers new regulations here, we offer two comments:

1. **We were pleased to see the SEC call for the use of strong "authentication measures that require users to present a combination of two or more credentials for access verification."**

   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 11.77 Billion "pwned" accounts representing more than 847 Million real world passwords exposed in data breaches. It is a security imperative for the United States to reduce the use of passwords alone for authentication and shift businesses and consumers to multi-factor and/or passwordless authentication.

2. **The SEC should consider strengthening its language on authentication to call for phishing-resistant authentication – in line with recent guidance from the White House and CISA.**

   We were pleased to see Footnote 40 in the draft regulations highlight the concerns about MFA methods that are based solely on SMS-delivery, and to see SEC note *"such methods may provide less security than other non-SMS based multi-factor authentication methods."* As we detail below, however, the SEC should go farther – and specifically call for the use of phishing-resistant authentication, in line with recent guidance from the White House and CISA.

   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.

   Unfortunately, the SEC's guidance here on use of other non-SMS authentication methods does not go far enough. 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:

   > *"MFA will generally protect against some common methods of gaining unauthorized account access, such as guessing weak passwords or reusing passwords obtained from a data breach. However, 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."*

   The White House has 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 <u>any</u> authenticator based on shared secrets can be compromised through phishing attacks.

   For this reason, the White House Strategy states: *"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.*

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

> *"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."*

The SEC should adjust the language in this 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[3] earlier this year, stating

> *"FIDO stands for "Fast IDentity Online" and is considered the gold standard of multi-factor authentication."*

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.[4]

We greatly appreciate the SEC's consideration of our comments. We look forward to further discussion with SEC 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 SEC staff officials desire to learn more about how FIDO authentication and how its certification programs work.

Please contact our Executive Director, Andrew Shikiar, at [redacted], or our government engagement advisor, Jeremy Grant, at [redacted].

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

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