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

Revised Proposed 2nd Amendment to Regulation 23 NYCRR 500 –Cybersecurity Requirements for Financial Services Companies

August 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 – Revised Proposed 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/

And from a security perspective, the imperative to move to adoption of phishing-resistant authentication is becoming more important than ever. As the July 24, 2023 report on the Lapsus$ group attacks from the U.S. Department of Homeland Security's Cyber Safety Review Board (CSRB)[2] noted:

> *The Board recommends that organizations urgently implement improved access controls and authentication methods and transition away from voice and SMS-based MFA; those methods are particularly vulnerable. Instead, organizations should adopt easy-to-use, secure-by-default, passwordless solutions such as Fast IDentity Online (FIDO)2-compliant, phishing-resistant MFA methods. Device and software manufacturers will need to innovate and deliver effective solutions that the global digital ecosystem can quickly adopt. To facilitate the transition to passwordless authentication, the Board recommends that the federal government develop and promote a secure authentication roadmap for the nation. The roadmap should include standards, frameworks, guidance, tools, and technology that can enable organizations to assess, progress, and implement leading practices for passwordless authentication.*

We have twice submitted comments to DFS as it considers new Cybersecurity Requirements for Financial Services Companies, and will not repeat all of our earlier comments here.

However, we are submitting this letter to flag a concern with a factual inaccuracy with regard to a statement in the assessment of public comments, as it relates to our suggestion that 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).

Per page 56 of the DFS assessment:

> Comment: One commenter stated that the Department should require phishing-resistant MFA for privileged accounts in line with recent guidance from the White House, CISA, and the Consumer Financial Protection Bureau ("CFPB"). According to this commenter, the current proposed language conflicts with language on MFA from the Department's investigation reports and guidance from CFPB and CISA and these reports noted there were problems with using app-based MFA and encouraged the use of physical security keys. This commenter further mentions that NIST's refreshed Digital Identity Guidelines (SP 800-63) will include language to differentiate phishing-resistance authentication from legacy MFA tools that are susceptible to phishing.
>
> Response: The Department encourages all covered entities to adopt phishing-resistant MFA where appropriate. Although physical security tokens, such as personal identity verification ("PIV") cards and security keys, offer phishing resistance, the Department believes **it will be too costly and burdensome** (our emphasis) at this time to require only phishing-resistant MFA for all covered entities. Therefore, the Department did not make any changes in light of this comment.

We have two specific concerns about this response:

1) **It assumes that all phishing-resistant MFA requires a standalone security token.**

   While physical security keys are one of the most frequently used form factors to deliver FIDO authentication – and a physical smart card is needed to deploy PIV cards – FIDO authentication is also frequently deployed through the use of "platform authenticators" which leverage the internal capabilities of smartphones, tablets, PCs, and laptops.

   Platform authenticators allow for end-users to make use of FIDO – frequently passwordless – without any external hardware. Instead, authentication is delivered by leveraging secure isolated execution environments common in computing devices today, such as Trusted Platform Modules (TPMs) in PCs and laptops, Trusted Execution Environments (TEEs) in Android devices, and Secure Enclaves (SEs) in Apple devices.

   When the White House Zero Trust Strategy stated that FIDO authentication "*is supported today by nearly every major consumer device,*" it was specifically referring to this fact.

[2] See https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

As one example of where FIDO authentication is frequently being deployed without separate hardware in the enterprise space, Microsoft's "Windows Hello for Business" solution has been used by thousands of companies to deliver passwordless, phishing-resistant authentication using the FIDO standards.

Put another way: we believe many of the devices financial services firms are using today support FIDO authentication without the need for a stand-alone device like a security key.

FIDO Alliance would welcome the opportunity to conduct a briefing with DFS staff if it would be helpful to learn more about the different types of options and form factors that can be used to deploy FIDO.

2) **DFS's assertion that "it will be too costly and burdensome at this time to require only phishing-resistant MFA for all covered entities" does not align with evidence we are seeing in the marketplace – including studies published both by end-users of FIDO, as well as independent market research and analysis firms.**

There are a number of studies documenting that a shift to phishing-resistant MFA not only does not create new cost or burdens for implementing organizations, but in fact leads to cost savings and other efficiencies.

- Google in 2016 published a case study documenting the results of their internal implementation of FIDO security keys.[3] Highlights:
    - Employees saved time each day, as it took them half as long to log in with FIDO as it did with the one-time password (OTP) solution FIDO replaced
    - Help desk calls tied to authentication problems plummeted to near-zero; Google stated "Our support organization estimates that we save thousands of hours per year in support cost by switching from OTP to Security Key."
    - There has not been a successful phishing attack against their 85,000+ employees since requiring use of physical security keys – given that a successful phishing attack could lead to millions of dollars in remediation costs, FIDO authentication has led to significant cost savings.
- Forrester Research this year published two studies that showed that a global company based in North America with 5,000 users and revenue of $2.5 billion per year would realize benefits of $4.8 billion over three years by deploying FIDO security keys[4], as well as similar benefits deploying FIDO platform authenticators instead of security keys.[5] Much of the benefit was derived from help desk support savings, security operations efficiency, and enhancements to end-user productivity.

In summary: while we understand that DFS may not be ready to follow other regulators in calling for the use of phishing-resistant authentication, we believe it is important that this decision be made with a full consideration of the facts available, both around FIDO form factors and delivery models, as well as around costs and burdens associated with a migration to the use of FIDO MFA.

If it would be helpful for us to present an overview of FIDO standards and the FIDO Alliance so that DFS staff officials can learn more about how FIDO authentication and the wide range of different form factors and delivery models that are used to support FIDO implementations, please let us know.

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.

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

[3] Google's case study was presented at a conference; see http://fc16.ifca.ai/preproceedings/25_Lang.pdf

[4] See https://tools.totaleconomicimpact.com/go/yubico/yubikeys/?lang=en-us

[5] See https://www.hypr.com/resources/report-forrester-tei-of-hypr