FIDO Alliance Input to the Consumer Financial Protection Bureau

ANPR on Consumer Access to Financial Records

February 2021

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the Consumer Financial Protection Bureau's (CFPB) Advance Notice of Proposed Rulemaking (ANPR) on Consumer Access to Financial Records, Docket No. CFPB-2020-0034.

The FIDO Alliance is a multi-stakeholder, public-private, industry standards development organization comprised of more than 250 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, 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 FIDO standards are being used across banking, payments, fintech, health care, government, enterprises, and e-commerce to deliver authentication that is both more secure and also easier to use.

Note that our members include both traditional financial institutions and fintech firms, and the broader discussion on this topic is one where our members, given their diversity, may have a diversity of views. For this reason, our comments on the draft are limited to those areas that touch on authentication and the security of systems that enable consumer access to financial records. Likewise, rather than respond to specific CFPB questions from the ANPR, we have chosen to frame our response at a higher level – focusing in on authentication as a fundamental building block to enable secure consumer access to financial records.

We offer four key points:

1. **Password-based systems for enabling information sharing create risks for consumers and financial services firms alike – and undermine other government and industry cybersecurity efforts.**

   Per page 22 of the ANPR, *"Consumers have an interest in being able to secure data access as provided in sec 1033 effectively and in a manner that enables ongoing and efficient consumer-friendly market innovation."*

There is nothing about a password-based approach to securing third-party access to consumer financial records that is consistent with this statement. Passwords aren't secure. They aren't consumer-friendly. And they aren't innovative. Moreover, when passwords are shared to enable third parties to access data via "screen scraping" approaches, they create additional risks.

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 10.5 Billion "pwned" accounts representing more than 613 Million real world passwords exposed in data breaches. Given how many consumers reuse passwords across sites, it is a security imperative for the United States to reduce the use of passwords alone for authentication and shift consumers to multi-factor and/or passwordless authentication.

Moreover, reliance on password-based screen-scraping approaches undermines broader national efforts to prevent phishing attacks. Industry and government invest millions of dollars each year on anti-phishing campaigns with a core message: "Don't ever share your passwords. And be especially sure not to share your banking password that's how you lose all your money."[1] The Federal Trade Commission (FTC) specifically tells people "Legitimate companies will not ask you for your password."[2]

Despite this, dozens of services have been built on an architecture whose core premise is to specifically ask consumers to share their passwords.

The dangers of this were documented in 2019 by FinCEN, when its Director Kenneth Blanco said:

> *"FinCEN has also seen a high amount of fraud, including automated clearing house (ACH) fraud, credit card fraud, and wire fraud, enabled through the use of synthetic identities and through account takeovers via fintech platforms. In some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires.*
>
> *"By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms' integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts. Some criminals are also monetizing stolen credit card information through fraudulent merchant accounts to charge victims' cards, or are simply creating fraudulent user accounts on fintech platforms as part of identity theft or synthetic identity fraud."*[3]

An additional challenge with any approach that relies on password-based screen-scraping is that it may undermine financial industry efforts to secure customer accounts with MFA. While passwords may be shared, possession-based authentication factors such as those using the FIDO standards are not shareable; the private key used to enable high assurance authentication is stored securely in the authenticator and cannot leave that device. Likewise, any MFA relying on an OTP with each login would require the consumer to provide that code each time an aggregator seeks to access account information. MFA is a security best practice whose use should be encouraged by regulators, but it is incompatible with screen-scraping approaches where third parties seek to obtain and cache authentication information.

Going forward, any approaches to third party access should focus on incenting all stakeholders to move away from insecure approaches based on password sharing and to instead build systems around secure APIs that embrace strong MFA.

[1] For example, see https://www.consumer.ftc.gov/blog/2016/02/trust-love-password-sharing and https://www.cisecurity.org/daily-tip/do-not-share-your-password/

[2] See https://www.consumer.ftc.gov/articles/0009-computer-security

[3] See Identity: Attack Surface and a Key to Countering Illicit Finance https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid

2. Attacks on some legacy types of MFA based off "shared secret" architectures have been increasing.

All MFA is not the same.

MFA adoption has been steadily increasing over the last 10 years – and with it, so have attacks seeking to defeat or circumvent MFA. Attackers have moved on to compromises of authentication tools that are also based on shared secrets, including both OTP and Push-based solutions. Here, we've seen a sharp increase in the number of phishing attacks looking to trick users into either handing over their OTP codes or pushing "approve" on a Push-based solution that has been activated as part of a phishing attack.

Google (a FIDO Alliance member) was one of the first to flag the problem, noting in 2015 that, a *"phisher can pretty successfully phish for an OTP just about as easily as they can a password"* and noted their shift to FIDO hardware-based solutions as the way to stop these targeted phishing attacks.[4] Note that Google had previously tried to drive two-factor login by offering OTP through both SMS and a free OTP app based on the OATH protocol; these comments reflected their experience with this technology.

2016 also saw what was perhaps the most visible and impactful phish of an OTP code, when the U.S. election was disrupted when Clinton campaign chair John Podesta's OTP-protected account was phished by the Russian government.

Since that time, the ability of adversaries to successfully phish OTP has only increased. Free, open source tools like Evilginx are easily available to anyone looking to phish a shared-secret-based authentication factor.[5] Per the release notes for Evilginx 2:

> *"Evilginx, being the man-in-the-middle, captures not only usernames and passwords, but also captures authentication tokens sent as cookies. Captured authentication tokens allow the attacker to bypass any form of 2FA enabled on user's account (except for FIDO U2F)."*[6]

OTP is routinely phishable, as attackers have figured out ways to phish OTP codes from users. Attackers have also found ways to phish authentication based on push notifications. If attackers can trick users into typing in a password, they can also trick them into sharing a six digit code or clicking "approve" on a push-based authentication app. This vulnerability was highlighted by the New York Department of Financial Services recent "Twitter Investigation Report" into the July 15, 2020 incident, where they wrote:[7]

> *"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."*

As a result, leaders in the security community have begun to move away from OTP and other authentication tools based on "shared secrets." Industry is shifting toward "high assurance" MFA where at least one factor is based on public key cryptography, and thus cannot be phished. Authentication using the FIDO standards is one such example.

---

[4] See https://www.youtube.com/watch?v=UBjEfpfZ8w0

[5] See https://github.com/kgretzky/evilginx2

[6] See https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/. Note that while Evilginx is formally published as a tool for researchers, it and many other similar tools can be used for nefarious purposes.

[7] Full report is at https://www.dfs.ny.gov/Twitter_Report

As part of any regulatory action, the CFPB should ensure that any MFA used to enable third party access to consumer financial data is "high assurance" MFA that can defeat these common attacks.

This is not a heavy lift for industry: as we outline in the next two points, the financial services industry has already created a standard API and a security architecture that integrates FIDO standards to deliver high assurance MFA in a way that is not only more secure than legacy approaches like OTP, but also easier for consumers to use.

3. **FIDO Authentication has been embraced by government and industry as the preferred way to deliver high assurance MFA to consumers.**

FIDO Alliance's work to standardize the use of on-device biometric matching coupled with authentication certificates using public key cryptography has transformed the identity and authentication market, creating a standards-based alternative to legacy authentication tools such as central-match biometric systems, one-time passwords (OTPs) and traditional PKI.

The increasing ubiquity of FIDO support in commercially available smartphones and other computing devices presents financial institutions, aggregators and fintech firms with new options for consumer authentication that improve security, privacy and usability.

FIDO is a global standard supported by every major platform

Over the last five years, the global leaders in security, technology, banking, payments, health care, telecommunications, and government that collectively comprise the FIDO Alliance has delivered a comprehensive framework of open industry standards for multi-factor authentication (MFA) that addressed key security and usability shortcomings in previous MFA tools, and that provide practitioners with new options for crafting digital identity solutions.

FIDO standards have delivered improvements in online authentication by means of open, interoperable technical specifications that leverage proven public key cryptography and on-device match of biometrics for stronger security and device-based user verification for better usability. The impact of FIDO standards, and formal certification testing to those standards, is notable:

- Firms including Google, Microsoft, PayPal, Apple, Amazon, Verizon, Facebook, ING Bank, Bank of America, USAA, Aetna, Intuit, Cigna, eBay, Dropbox, Salesforce and their peers around the world have deployed authentication solutions based on the FIDO standards; .
- Governments around the world that are either using FIDO today for citizen identity or have announced plans to modernize citizen identity systems around a FIDO-centric architecture include Korea, Thailand, Taiwan, the United Kingdom, and the United States. In the U.S., the Login.gov service has adopted FIDO authentication to protect accounts used to access a variety of citizen-facing services. And CISA has advised election officials to adopt FIDO security keys.[8]
- The W3C has finalized a formal new Web Authentication standard (WebAuthn)[9] that is part of the FIDO2 standards. This standard enables FIDO functionality to be embedded in major browsers (i.e., Chrome, Edge, Firefox, Safari) – meaning that FIDO-standard MFA can be deployed for any web application without any significant burden on the part of an implementer. As of January 2021, over 86% of browsers in use have built-in support for FIDO through support of WebAuthn.

[8] See https://www.cisa.gov/sites/default/files/publications/CISA_Insights_Actions_to_Counter_Email-Based_Attacks_on_Election-Related_S508C.pdf

[9] See https://www.w3.org/TR/webauthn/

- The ITU has formally adopted the FIDO specifications as standards, through ITU X.1277 (FIDO Universal Authentication Framework) and ITU X.1288 (FIDO Client to Authenticator Protocol (CTAP)/Universal 2-factor Framework)
- More than 750 products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.
- Core device platforms have also become FIDO Certified, leading to smartphones and laptops where FIDO Authentication is built in natively into browsers and platforms – meaning that neither implementers nor their customers need to buy a separate technology to enable MFA.

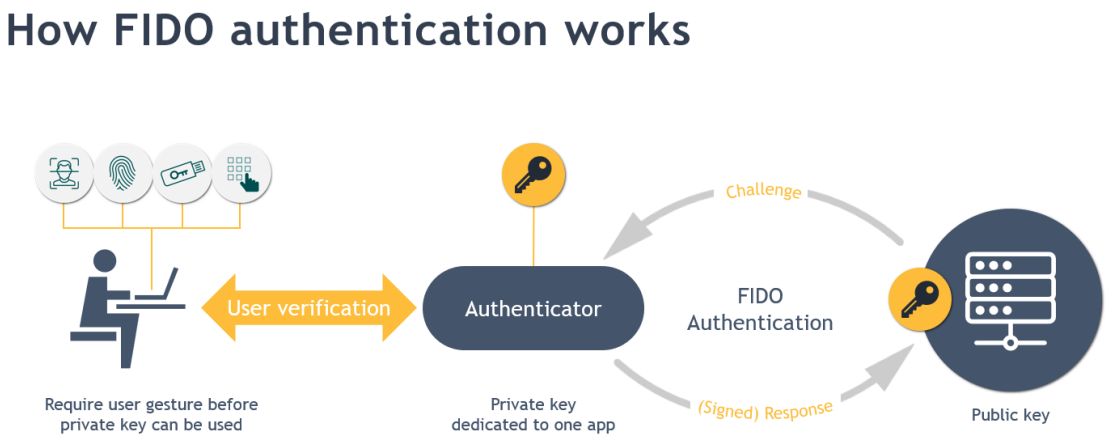
  For example, Microsoft has embedded FIDO at the OS level in Windows 10, where it provides the basis for the Windows Hello passwordless login solution.[10]

  And, Google has embedded support for FIDO in at both the OS level (Android) and the browser (Chrome) – all devices running Android 7 and above (more than 1 billion in total across the globe) are now FIDO Certified to serve as authenticators.[11]

  All told, we estimate that well over 2.5 billion devices on market today have built-in support for FIDO Authentication.

How FIDO Works

At its core, FIDO Authentication is based on the use of use of authentication certificates using asymmetric public key cryptography. Authentication keys can either be standalone "Security Key" devices or embedded inside devices like laptops or smartphones. Regardless of the form factor, a FIDO authenticator requires that the user makes some sort of gesture – touching the key, matching a biometric, or authenticating a PIN – before the private key can be used.



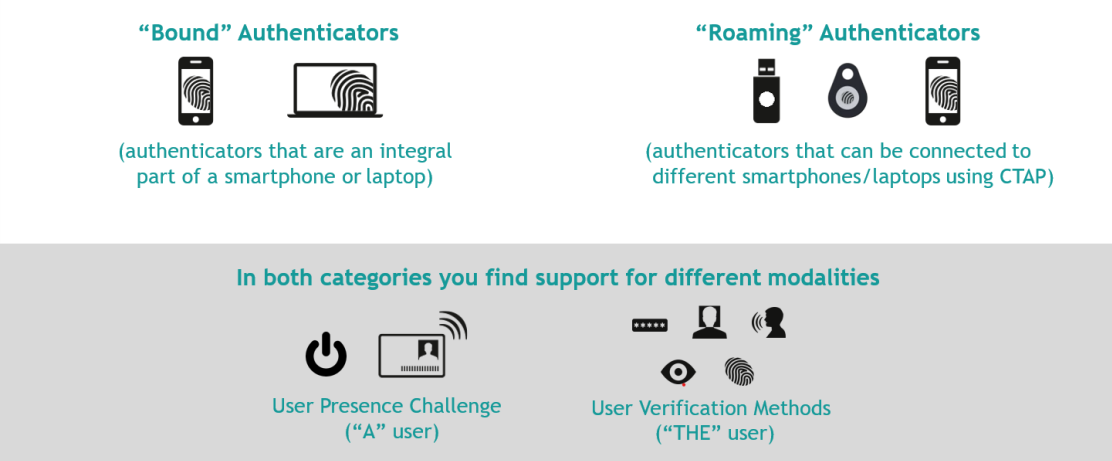
Sometimes FIDO Authentication is used as a second factor to augment passwords – this is how it is commonly used in the "Security Key" model popularized by Google and other firms.

[10] More details on the Microsoft announcement are at https://www.microsoft.com/en-us/microsoft-365/blog/2018/11/20/sign-in-to-your-microsoft-account-without-a-password-using-windows-hello-or-a-security-key/

[11] More details on the Google announcement are at https://threatpost.com/google-ditches-passwords-in-latest-android-devices/142164/

Sometimes FIDO Authentication is used to provide two separate factors to enable a true "passwordless" experience. For example, patients log into Aetna's smartphone app by first authenticating their fingerprint or face on the device; that biometric factor then unlocks the cryptographic key.

As the graphic below details, the introduction of the FIDO2 standards is creating additional ways to use FIDO Authentication, including ways that the secure hardware in smartphones themselves can be used as Security Keys.



4. **The good news: Industry has largely solved the "secure technical layer" to enable better consumer access to financial data – and industry-led efforts are improving every year.**

FIDO Alliance – together with the Financial Data Exchange (FDX) – have created industry standards that together can be used to enable secure third-party access to consumer financial accounts in a way that is secure, privacy-preserving, and easier to use than legacy password-based approaches.

- The FDX API has been created jointly by banks, aggregators, and fintech startups to enable a modern, standardized approach to enable consumers to grant third-party access to their financial data. Relative to screen scraping, the FDX API delivers much better security and privacy, including the ability for consumers to meaningfully authorize access to data on a granular level (allowing access to some data elements and not others), while also being able to easily revoke access if they choose. And because no passwords are exchanged or cached when the API is used, the risk model is much lower.
- FDX's "Control Considerations for Consumer Financial Account Aggregation Services" detail a reference security architecture for use of the FDX API by both financial institutions and third party aggregators. This architecture specifically highlights the use of FIDO authentication standards and details how FIDO standards should be used with the FDX API and other industry "best practice" standards such as OpenID Connect.

We have been encouraged by the broad support among financial institutions, aggregators, and fintech firms for FDX and its work. We note that there is some broader discussion and debate across industry as to whether other APIs should be used in addition to what FDX has crafted, and we are not opposed to the use of additional APIs.

Likewise, there are other secure approaches to authentication – such as PKI – that do not make use of the FIDO standards. However, we suggest that any API or authentication approach used should ideally demonstrate a comparable level of security to the FDX architecture in order to prevent attacks commonly executed against weaker authentication tools. Such an approach will ensure that any regulatory efforts involving consumer access to financial records improve security and privacy for consumers.

We greatly appreciate the CFPB's consideration of our comments. We look forward to further discussion with the CFPB 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 CFPB staff desire to learn more about how FIDO authentication works.

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