FIDO Alliance Input to the Consumer Financial Protection Bureau

Small Business Advisory Review Panel on Required Rulemaking on Personal Financial Data Rights

January 2023

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment to the Consumer Financial Protection Bureau's (CFPB) as CFPB conducts its Small Business Advisory Review Panel for Consumer-Permissioned Sharing of Consumer Financial Data.

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.

FIDO Alliance members include companies of all sizes, from small fintech and security startups to some of the world's largest companies. 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. We were pleased to see CFPB recognize the importance of FIDO standards – specifically the FIDO2 Web Authentication standard – in its August 2022 Consumer Financial Protection Circular 2022-04, which noted *"MFA solutions that protect against credential phishing, such as those using the Web Authentication standard supported by web browsers, are especially important."*[1]

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. We also recognize that implementation timelines for requirements will differ based upon institutional size and therefore, make no comments on how this is approached. Likewise, rather than respond to every CFPB question from the proposal, we have chosen to limit our response to those questions that relate to work relevant to FIDO Alliance – focusing in on authentication as a fundamental building block to enable secure consumer access to financial records.

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

Before diving into the specific questions posed by CFPB, 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.**

   As CFPB flagged in its 2020 ANPR on this topic, *"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 12.2 Billion "pwned" accounts representing more than 847 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: Never share your passwords.[2] The Federal Trade Commission (FTC) has specifically told people "Legitimate companies will not ask you for your password."[3]

   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."*[4]

   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, as well as CFPB's own direction to financial institutions on MFA use in Circular 2022-04. Indeed, given that this Circular suggested a lack of MFA could create liability for financial institutions, any regulatory path where CFPB allows credential caching and screen-scraping would seem to conflict with CFPB's own guidance.

---

[2] For example, see https://www.justice.gov/usao-ndga/protecting-yourself-while-using-internet and https://www.consumer.ftc.gov/blog/2016/02/trust-love-password-sharing and https://www.cisecurity.org/daily-tip/do-not-share-your-password/

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

[4] 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

While passwords may be easily shared with third parties – enabling sharing of data through screen scraping – possession-based authentication factors such as those using the FIDO standards cannot. 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.

With regard to the impact of such a change on small businesses: a consistent theme that security experts have seen over the last twenty years is that small businesses often struggle with cybersecurity, in that they do not have the resources to properly secure critical assets – passwords among them.[5] This is one reason why, year after year, attacks that leverage compromised passwords are the leading attack vector used to perpetrate cybercrime. Any financial data ecosystem that relies on passwords as a critical security layer is thus highly likely to put small businesses in financial services and their customers at additional risk; a shift to more secure APIs can help to mitigate that risk.

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.[6] 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.[7] 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)."*[8]

[5] See https://www.forbes.com/sites/edwardsegal/2022/07/13/why-small-and-medium-companies-face-more-cyber-challenges-than-large-ones-survey/

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

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

[8] 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.

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. These so-called "MFA Fatigue" attacks sharply increased over the last year, with firms like Uber and Twilio falling victim to these attacks. A notable exception here was Cloudflare, who documented that their use of FIDO security keys allowed them to defeat these attacks.[9]

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. CISA has called FIDO the "gold standard" of MFA and urged industry to embrace FIDO authentication over other MFA tools.[10] And as noted earlier, CFPB in Circular 2022-04 flagged the importance of the FIDO Web Authentication standard.

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.

<u>FIDO is a global standard supported by every major platform</u>

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.

[9] See https://www.protocol.com/bulletins/uber-breach-hacker-twilio-mfa

[10] See https://www.cisa.gov/blog/2022/10/18/next-level-mfa-fido-authentication

- 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. The White House has required phishing-resistant authentication across all government services as part of its Zero Trust Strategy and specifically called out the importance of the FIDO standards in achieving this goal.[11] And CISA has advised election officials to adopt FIDO security keys.[12]
- The W3C Web Authentication standard (WebAuthn)[13] 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.
- More than 900 products have been FIDO® Certified – demonstrating a mature, competitive, interoperable B2B ecosystem of authentication and identity solutions.
- Core device platforms from Apple, Google, and Microsoft all support FIDO authentication out of the box, meaning that nearly every commercially available smartphone and laptop has support for FIDO Authentication built in natively into browsers and platforms – meaning that neither implementers nor their customers need to buy a separate technology to enable MFA.

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.

[11] See https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[12] See https://www.cisa.gov/sites/default/files/publications/CISA_Insights_Actions_to_Counter_Email-Based_Attacks_on_Election-Related_S508C.pdf
[13] See https://www.w3.org/TR/webauthn/

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.

Below we offer additional inputs based on specific questions in CFPB's Outline of Proposals and Alternatives Under Consideration:

Questions on Direct Access

Q39. Please provide input on the approach the CFPB is considering with respect to requiring covered data providers to make information available directly to consumers if they have enough information to reasonably authenticate the consumer's identity and reasonably identify the information requested. What alternative approaches should the CFPB consider?

In 2023, there is no longer any such thing as a "secure" password, and there should be no confidence that use of a password alone provides enough information for a firm to "reasonably authenticate the consumer's identity." Nevertheless, passwords persist in the financial services ecosystem, as it is taking time for financial services firms to migrate to stronger forms of authentication.

One challenge that CFPB should consider is that any regulation that allows for the continued use of password-based screen scraping creates additional risks for consumers and financial services firms alike. In that today, a compromised password may grant an attacker access to certain elements of a consumer's financial data, but if new regulations allow the holder of a password to access additional data elements tied to a consumer's account, then a compromised password would become more valuable. This is another reason why getting the authentication layer right is essential to protecting consumer financial data.

Q46. How do covered data providers authenticate a consumer's identity when making information available other than through an online financial account management portal?

Today that answer varies across the industry. Some financial intuitions have adopted FIDO authentication or other MFA for consumer authentication; some are still using nothing but passwords, and some might be using a mix of different authentication technologies, including the use of data analytics and behavior analytics tools that complement traditional authentication tools.

A challenge that many FIDO members in the financial services sector have articulated is that the continued existence of third parties that access consumer financial data through screen scraping is inhibiting MFA adoption, since the screen-scraping tools break when MFA is turned on. Some financial services firms have looked to "MFA bypass" tools as a work-around to allow authorized third parties to continue to screen scrape with cached credentials, but as password-based cyber-attacks on financial services firms escalate each year, the risk involved with use of these tools has become untenable.

Moreover, as financial services firms look to embrace passwordless MFA experiences using tools like the FIDO standards – which can entirely eliminate passwords from the consumer authentication process – there is no way those tools can be made to work with screen scraping. Eliminating screen scraping and pushing industry to adopt APIs is thus of critical importance, as it will make it easier for financial services firms to adopt more modern, secure approaches to authentication that do not involve passwords.

Questions on Third Party Access

Q50. Please provide input on the approach the CFPB is considering with respect to the third-party access portal proposal. What alternative approaches should the CFPB consider?

We believe the CFPB is right when it says it is "concerned that screen scraping presents some significant limitations and risks to consumers, data providers, and third parties, including risks related to possession of a consumer's credentials," and that "making information available through a third-party access portal that does not rely on an authorized third party possessing or retaining consumer credentials to authenticate the authorized third party could enhance consumer privacy, data security, and data accuracy, and promote the development and use of standardized formats for information."

Q55. Should covered data providers be required to permit screen scraping when the covered data provider's third-party access portal experiences a service interruption? What records could demonstrate that a service interruption to a third-party access portal has occurred? What alternatives to screen scraping should the CFPB consider to reduce interruptions to authorized third party information access when a third-party access portal experiences a service interruption?

No. The idea of a "fallback" option is interesting, but the overwhelming interest here should be to eliminate passwords and encourage MFA, per the CFPB's August 2022 guidance. But screen scraping doesn't work with MFA or passwordless solutions – and if covered data providers are being told they need to support screen scraping as a fallback option, that would require that they turn off MFA and passwordless solutions and revert back to use of passwords. That's not a viable option.

Q56. To the extent screen scraping is a method by which covered data providers are permitted to satisfy their obligations to make information available, how could the CFPB mitigate the consumer risks associated with screen scraping? For example, should the CFPB require covered data providers to provide access tokens to authorized third parties to use to screen scrape so that third parties would not need a consumer's credentials to access the online financial account management portal? Alternatively, should authorized third parties be restricted from retaining consumer credentials indefinitely? For how long do authorized third parties need to retain consumer credentials? If the answer depends on the use case, please explain.

To the point above, we do not think screen scraping can be made secure. The best thing the CFPB can do here is push all firms in the financial services ecosystem to embrace APIs.

Q57. Please provide input on whether CFPB-defined standards are needed to promote the availability of data to authorized third parties, whether certain aspects of the regulation of third-party access portals are better suited to be regulated by industry participants, and how the CFPB can promote the development of industry standards. How should the CFPB take account of the voluntary standards and guidelines that some industry participants have developed as the CFPB is considering regulating third-party access portals?

We do not believe that CFPB should look to define standards itself; doing so would only set back efforts to open up the consumer financial data ecosystem by years. It will be much more effective for CFPB to point to existing industry standards, allowing the government to leverage the good work that has been done in the private sector to develop solutions to tackle the objectives CFPB is pursuing. Most of the hard work has been done here already in standards organizations like FDX, the Open ID Foundation, FIDO Alliance, and the W3C.

If there are use cases where CFPB believes that a voluntary industry standard does not meet a CFPB outcome or goal, CFPB can let those groups know – and ask them to collaborate to revise or augment those standards, rather than create their own. FIDO Alliance, for example, has an active Government Deployment Workgroup where industry and government collaborate; it's a place for agencies to share use cases and for FIDO to then work on solutions to address them. CFPB would be welcome to participate in FIDO Alliance as part of the US government's membership in the organization.

Questions on Security of Third Party Access portals

Q69. Please provide input on the approach the CFPB is considering with respect to the security of a covered data provider's third-party access portal. What alternative approaches should the CFPB consider?

CFPB has stated it is considering a proposal in which the third-party access portal could not rely on an authorized third party possessing or retaining a consumer's credentials to authenticate the authorized third party. FIDO Alliance supports this. As we have noted previously, any tool that relies on passwords – and caching credentials – is flawed, and only undermines the security of the financial services ecosystem. By looking to regulations that embrace the use of APIs – ideally secured with FIDO authentication – to manage connections between covered data providers and third parties, CFPB can ensure that there is a strong foundation in place for enabling consumers to easily and securely share their personal financial data.

Q70. What methods of securely authenticating an authorized third party do not require consumers to share their credentials with the authorized third party? Should the CFPB consider proposals to articulate performance standards related to authentication? If so, how should the CFPB address such topics?

As noted earlier, secure authentication that does not rely on sharing credentials is happening each day with millions of transactions through APIs such as the FDX API.

With regard to performance standards for authentication, we suggest that CFPB reiterates its guidance from 2022 that financial institutions should be using phishing-resistant authentication.

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.