FIDO Alliance Comments to the U.S. Department of the Treasury

October 2025

Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets

The Fast Identity Online (FIDO) Alliance appreciates the opportunity to provide input to the Department of the Treasury on its *Request for Comment (RFC) on Innovative Methods To Detect Illicit Activity Involving Digital Assets.*

As background, 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, cryptocurrency, fintech, and payments – as well as those many of the security vendors those firms turn to when it comes to guarding against attacks on identity verification and authentication.

1Password
amazon
AMERICAN EXPRESS
Bank of America
BEYOND IDENTITY
CHASE
CISCO
CVSHealth
Daon
DASHLANE
DELL
egis Technology
FEITIAN WE BUILD SECURITY
Google
HYPR
IDEMIA PUBLIC SECURITY
infineon
INTUIT
LastPass
Lenovo
LINEヤフー
mastercard
mercari
Meta
Microsoft
NTT docomo
okta
OneSpan
PayPal
PNC BANK
Prove
RAON
RSA
SAMSUNG
sto
swissbit
THALES
TikTok
usbank
VISA
WELLS FARGO
yubico

The launch of the FIDO Alliance in 2012 – and the subsequent creation and mass adoption of FIDO authentication standards over the eleven 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 FIDO standards have emerged as the de-facto best choice for implementers seeking to deploy phishing-resistant authentication – such as passkeys and security keys – that are both more secure and also easier to use than legacy authentication tools.

FIDO Alliance has also launched a number of industry-first programs to test and certify the performance of different technologies used in remote identity-proofing, such as biometric tools and document authentication tools used by financial services firms to help satisfy Customer Identification Program/Know Your Customer (CIP/KYC) requirements.

Of note, FIDO's standards and certification programs covering authentication and identity proofing have been designed, in part, with input from U.S. government agencies. Both NIST and Treasury participate in FIDO Alliance, along with a number of other Federal agencies, including the GSA, VA, and Department of Defense. The ability to get real-time input from public-sector members as FIDO Alliance creates new initiatives has been very helpful in ensuring that our deliverables are able to help address technical, business, policy, and regulatory challenges from government partners.

As we detail in our comments, FIDO Alliance's standards and certification programs offer Treasury a set of tools that Treasury and the financial services sector can leverage in order to help address concerns about illicit finance in the digital assets space.

Given the increasing role that compromises of identity and authentication play in illicit activity in digital assets, we were pleased to see Congress direct Treasury to focus on digital identity issues in this RFC. Analyses and alerts from agencies like FinCEN[1] and the Department of Justice;[2] have made it increasingly clear that weak identity and authentication solutions present a serious problem in enabling financial crimes – with the primary beneficiaries being hostile nation-states and organized crime gangs.

Against this backdrop, we are now seeing the rise of new, more sophisticated attacks on identity such as AI-powered deepfakes that, if unaddressed, threaten to push losses from identity-related cybercrime and other illicit activity to new levels and undermine confidence in our increasingly digital economy.

Given the focus of FIDO Alliance on identity and authentication issues, we are limiting our responses to a subset of questions on this topic from the RFC.

Question 4. What innovative or novel methods, techniques, or strategies related to digital identity verification are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to digital identity verification? Please describe the portable digital identity credentialing tools in use and how such tools are being used.

At a high level, we are seeing financial institutions, technology companies, and third-party service providers leveraging a variety of tools to detect illicit activity and/or mitigate potential illicit finance risks. These include multi-layered, advanced digital identity solutions that make use of tools including:

- **Remote document authentication and "selfie-match" technologies.** On the identity proofing side, many of our members have augmented or replaced knowledge-based verification (KBV) tools which have been traditionally used to support CIP requirements in remote account opening with newer technologies, such as those that ask a customer to take a photo of their driver's license, state ID card, or passport, and then submit a "selfie" photo. These solutions analyze whether the credential appears to be legitimate, as well as whether the photo on the ID matches the selfie (by conducting a 1:1 biometric verification against the photo on the credential). These tools are also often used to support account recovery processes as a safeguard against Account Takeover (ATO) attacks – to verify that someone who claims to be locked out of their account is in fact that person and not an impostor.

[1] See https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf and https://www.fincen.gov/sites/default/files/2024-06/PREPARED-REMARKS-IDENTITY-PROJECT-COLLOQUIUM-FINAL-508_0.pdf

[2] See https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targetingperceived andhttps://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commitcyberattacks-and and https://www.reuters.com/article/world/north-korea-took-2-billion-in-cyberattacks-to-fund-weaponsprogram-un-report-idUSKCN1UV1ZX/ and https://www.fbi.gov/wanted/cyber/dprk-it-workers

Performance varies significantly among different products; this has been documented by DHS's Science and Technology Directorate, which has launched a program to test their performance.[3]

In response to industry concerns about the varying levels of reliability among these products, the FIDO Alliance has launched a first-of-its kind, industry-led program that developed performance standards for both document authentication and selfie-match face verification tools. The Alliance has partnered with a number of accredited test labs to test and certify that products meet expected performance requirements.[4]

Notably, NIST embraced FIDO Alliance's performance standards for remote document authentication as a condition of meeting Identity Assurance Level 2 (IAL2) in its most recent update of its Digital Identity Guidelines, SP 800-63-4.[5]

As we note in our answer to question 4(d) below, we believe Treasury and other regulators should consider referencing use of FIDO certified remote identity verification products as one way for firms in the digital assets space to reduce risks associated with illicit finance tied to compromised or synthetic identities.

- **Liveness detection for biometrics.** Generative AI has made it much easier for adversaries to create convincing fake photos, voices, and videos, and many firms are finding themselves in an arms race with these adversaries to counter the new attacks. The use of liveness detection technologies can help organizations determine if a biometric sample comes from a live person or a modified or generated representation, and has become a best practice when biometrics are being captured in a remote setting. Many of the best tools that are being used for liveness detection make use of AI themselves.

  Of note, FIDO Alliance's certification program to test and certify the performance of remote biometric identity verification technologies requires vendors to demonstrate their ability to detect a live face from an adversary that is looking to spoof a face.

- **Phishing-resistant authentication rooted in public key cryptography.** Phishing attacks that are focused on stealing both passwords and multifactor authentication (MFA) codes have been on the rise in recent years; the FinCEN report we referenced earlier noted that *"18%, or approximately 446,000 identity-related BSA reports, report that attackers used compromised credentials to gain unauthorized access or misused their authorized access to generate illicit proceeds. Compromises are disproportionally costly as they accounted for 32% of the total suspicious activity amount or $112 billion."*

  Moreover, Treasury, CISA, and the FBI have previously reported that North Korean state-sponsored actors are targeting the authentication tools used to protect cryptocurrency accounts and leveraging compromised credentials to steal billions of dollars to fund their weapons programs.[6]

[3] See https://www.dhs.gov/science-and-technology/remote-identity-validation-rally

[4] See https://fidoalliance.org/fido-alliance-addresses-accuracy-bias-in-remote-biometric-identity-verification-technologies-industry-first-testing-certification-program/ and https://fidoalliance.org/certification/identity-verification/document-authenticity/

[5] See https://pages.nist.gov/800-63-4/sp800-63b.html

[6] See https://www.ic3.gov/CSA/2022/220418.pdf

Phishing attacks are now being supercharged by generative AI tools that significantly simplify the creation of compelling phishing campaigns at scale. This, in turn, is making it much easier for adversaries to compromise legacy MFA tools and creating an imperative to implement phishing-resistant authentication for users, such as tools that use PKI or the FIDO standards, both of which leverage asymmetric public key cryptography to block phishing attacks.

Within the cryptocurrency ecosystem, we have seen significant attention over the last few years around the importance of phishing-resistance – and with it, increased use of the FIDO standards for authentication. This has been driven in large part by a rash of cryptocurrency thefts that were enabled by weak authentication – specifically, attacks where adversaries phished OTP codes to take over accounts. Beyond using FIDO security keys (hardware keys) or passkeys on a mobile device to safeguard authentication, we are also seeing FIDO being use to provide additional protections for sensitive trades or transactions where "transaction signing" tied to a phishing-resistant credential rooted in public key cryptography is essential to delivering high assurance. With a strong signal that a trade confirmation step came from a known device and the user provided an intentional action (FaceID, fingerprint, or PIN) the chances of an illicit trade are greatly diminished.

Here we note that the emergence of passkeys (which enable phishing-resistant passwordless logins using the FIDO standards) is transforming the authentication landscape. For the first time, consumers can enjoy an authentication experience that does not require any password and that is much easier to use. On that front, NIST recently issued guidance making clear that passkeys meet Authentication Assurance Level 2 (AAL2) requirements for MFA and urging the use of phishing-resistant authentication "wherever practical."[7] However, despite the NIST guidance, we continue to hear from financial services firms that there is regulatory uncertainty about whether and when passkeys can be used. This is an area where clearer guidance from Treasury and the financial regulators would be most welcome.

4(b) How are financial institutions using digital identity verification tools in AML/CFT and sanctions compliance efforts in relation to other tools (*e.g.*, in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of digital identity tools with other existing or previous tools used for similar purposes.

As noted above, many financial services firms have embraced remote document authentication and "selfie-match" technologies as a way to augment or replace legacy knowledge-based verification (KBV) tools for both account opening and account recovery. We note that NIST first advised organizations not to use KBV for remote identity proofing in 2017, however its use persists across the financial services sector today.

To our point above, while remote document authentication and "selfie-match" technologies offer higher reliability relative to KBV, their performance still varies, and there is a need to point financial services firms to those tools that are at the high end of performance. The use of FIDO-certified remote identity verification products is one way for firms in the digital assets space to know they are using remote identity proofing tools that are proven in their ability to reduce risks associated with illicit finance tied to compromised or synthetic identities.

[7] See https://pages.nist.gov/800-63-4/sp800-63b.html

4(c) Are there regulatory, legislative, supervisory, or operational obstacles to using digital identity verification to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

As we noted above, despite NIST formally recognizing passkeys as meeting Authentication Assurance Level 2 (AAL2) requirements for MFA, we continue to hear from financial services firms that there is regulatory uncertainty about whether and when passkeys can be used. Much of this seems tied to the fact that passkeys are viewed by some examiners as a "new" authentication technology, and thus financial services firms are nervous as to whether they might face difficult questions from an examiner regarding their use of passkeys. This is an area where clearer guidance from Treasury and the financial regulators would be most welcome.

We note that the FDIC recently weighed in with new supervisory guidance on the use of pre-populated information for purposes of meeting Customer Identification Program (CIP) requirements,[8] which helped to clarify that financial institutions are allowed to use these solutions. A similar advisory from FDIC and other financial regulators – and the Treasury Department – would be most welcome.

4(d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets?

There are two steps the U.S. government can take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets

1) **Issue definitive guidance to financial services firms to encourage the use of phishing-resistant authentication and recognize the role that passkeys can play in enabling it.**

   As we noted earlier, we continue to hear from financial services firms that there is regulatory uncertainty about whether and when passkeys can be used.

   Likewise, financial regulators have largely been silent about the threat to legacy forms of MFA and the need to ensure that financial services firms use authentication technologies that can stand up to phishing attacks – even as we see a wave of successful attacks on cryptocurrency and traditional finance applications tied to a compromised password or OTP.

   In the time since the FFIEC last updated its "Authentication and Access to Financial Institution Services and Systems" guidance (in 2021), CISA,[9] NIST,[10] OMB,[11] and other government agencies have issued guidance on the importance of phishing resistance – all of which highlighted FIDO authentication as one of the best ways to achieve it.

   Additionally, FinCEN last year noted that *"18%, or approximately 446,000 identity-related BSA reports, report that attackers used compromised credentials to gain unauthorized access or misused their authorized access to generate illicit proceeds. Compromises are disproportionally costly as they accounted for 32% of the total suspicious activity amount or $112 billion."* [12]

   While we are not calling for FFIEC to shift away from the risk-based approach to authentication it has outlined in previous guidance, a FFIEC update that recognizes the importance of phishing-resistance,

[8] See https://www.fdic.gov/news/financial-institution-letters/2025/fdic-supervisory-approach-regarding-use-pre-populated

[9] See https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[10] See https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom and https://pages.nist.gov/800-63-3/sp800-63b.html

[11] See https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[12] See https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf

and/or a statement on the need of an authentication solution to guard against phishing attacks would be very helpful in driving the adoption of more resilient authentication solutions that can protect consumers from attacks tied to compromised credentials.

2) **Advise financial services firms to make use of FIDO-certified identity verification solutions**

As we noted earlier, the performance of document authentication and selfie-match tools used in remote identity verification varies significantly among different products, as documented by DHS's Science and Technology Directorate.

FIDO Alliance's first-of-its kind effort to develop performance standards for both document authentication and selfie-match face verification tools – and partner with a number of accredited test labs to test and certify that products meet expected performance requirements – has provided the financial services sector with a way to understand whether the tools they are using for remote identity verification in account opening and account recovery use cases meets critical performance metrics.

We believe Treasury and other regulators should consider referencing use of FIDO certified remote identity verification products as one way for firms in the digital assets space to reduce risks associated with illicit finance tied to compromised or synthetic identities. This would align the financial services sector with guidance from NIST, who (as we noted earlier), embraced FIDO Alliance's performance standards for remote document authentication as a condition of meeting Identity Assurance Level 2 (IAL2) in its most recent update of its Digital Identity Guidelines, SP 800-63-4.

We appreciate Treasury's considerations of our comments and suggestions. Should you have any questions on our submission – or would like to learn more about FIDO standards and certification programs – please reach out to our Executive Director, Andrew Shikiar, at andrew@fidoalliance.org, or our policy advisor, Jeremy Grant, at jagrant@venable.com.