Comments to the Department of the Treasury

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

October 2025

The Better Identity Coalition appreciates the opportunity to provide input to the Department of the Treasury on its *Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets.*

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 20 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, cryptocurrency, health care, technology, fintech, payments, and security.

Up front, we note that of our 20 members, roughly half are either financial institutions, fintech, cryptocurrency, or payments firms; many of our other members create the solutions that are used by these firms to vet, validate, and authenticate digital identity. This unique mix of members allows the Coalition to weigh in from the perspective both of the firms that will be most impacted by any new action from financial regulators, as well as those who be asked to deliver solutions to help these firms comply.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

In 2018, we published "Better Identity in America: A Blueprint for Policymakers" – a document that outlined a comprehensive action plan for the U.S. government to take to improve the state of digital identity. In the Blueprint, we specifically called on the Treasury Department and financial regulators to take a leadership role in driving the adoption of more resilient digital identity solutions across the financial services market. We published an updated version of this Blueprint in January with a set of recommendations for the new Administration, and which reiterated this point.

On this front, we have been encouraged by Treasury's recent work around digital identity – including highlighting the importance of digital identity in the Administration's recent report on Strengthening American Leadership in Digital Financial Technology.

With regard to this RFC, we believe the key point for Treasury to understand is that a significant portion of illicit activity in digital assets is tied to compromises of identity or authentication – and that the government has a significant role to play in addressing deficiencies in identity and authentication infrastructure that have made it easy for adversaries to perpetrate this fraud.

While exact statistics on illicit activity tied to identity are hard to come by, there are a set of reports from the U.S. government that together make clear that weak identity and authentication infrastructure presents a serious problem in payments fraud and other financial crimes.

- The Financial Crimes Enforcement Network (FinCEN) has noted that $212 billion worth of suspicious financial transactions in 2021 was tied to some form of identity compromise;[1] at a 2024 conference, they revealed that this number had exploded in 2023 - covering over 70% of all Suspicious Activity Reports (SARs) filed by banks, tied to $394 billion of transactions.[2]

- The Government Accountability Office (GAO) estimates that fraud losses cost the government $233 billion-$521 billion annually; GAO noted that pandemic unemployment insurance fraud losses alone totaled $100-135 billion, and that most of these losses were tied to identity fraud.[3]

- Chinese state-sponsored attackers have stolen billions through identity-centric attacks;[4] the Justice Department has noted North Korea stole more than $2 billion to fund its nuclear program through similar attacks targeted against banks and crypto exchanges,[5] and more recently spoofed identities to place North Koreans in remote IT jobs to generate additional money to fuel its weapons of mass destruction.[6]

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

[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] As detailed in a FinCEN speech at the 2024 Fed ID Forum – see https://events.afcea.org/FedID24/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=11005&SessionDateID=747
[3] See https://www.gao.gov/products/gao-24-105833 and https://www.gao.gov/blog/more-fraud-has-been-found-federal-covid-funding-how-much-was-lost-under-unemployment-insurance-programs
[4] See https://www.justice.gov/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targetingperceived
[5] See https://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/
[6] https://www.fbi.gov/wanted/cyber/dprk-it-workers

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.

Up front, it is worth noting that while financial services firms make use of many innovative and novel methods, techniques, and strategies related to digital identity, they are making very little use of "portable digital identity credentialing tools."

There are two primary reasons for this:

1) The portable digital identity credentialing tools that financial services firms are most interested in using – mobile driver's licenses (mDLs) and other verifiable digital credentials (VDCs) that aredigital counterparts to government-issued credentials such as state ID cards, passports, and social security cards – are not yet widely available in the market. Where mDLs are available today, their use is largely limited to in-person use cases (such as clearing a TSA checkpoint), however, they are not yet able to address the online use cases that could help to address major issues involving illicit activity in digital finance.

   As we note throughout our response, we believe that Treasury and the Federal government writ large have a significant role to play in 1) jumpstarting the availability of these credentials via grants to states, and 2) clarifying that these credentials are acceptable for use to meet BSA/AML requirements.

2) There are a number of companies that offer portable digital identity credentialing tools that have been certified as meeting NIST requirements for Identity Assurance Level 2 (IAL2).[7] However, financial services firms have, to date, not viewed those offerings as a good fit to meet their own business and regulatory requirements tied to new account opening.

   As we discuss later in our response, we believe Treasury and the prudential regulators should consider affirmatively stating that digital identity solutions that have been certified as meeting IAL2 (as defined by NIST's most recent update to its digital identity guidelines (SP 800-63-4) may be used by firms in the digital assets space to meet CIP requirements.

In terms of the tools used today: at a high level, we are seeing financial institutions, technology companies, and third-party service providers leveraging a variety of tools to

[7] Note that the Kantara Initiative is a non-profit organization that runs a certification program for identity providers to demonstrate their compliance with IAL2.

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 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). Performance varies among different products; DHS's Science and Technology Directorate has launched a program to test these products,[8] and the FIDO Alliance has launched an industry-led program that partners with accredited test labs to test and certify that products meet expected performance requirements.[9]

- 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, liveness detection technologies broadly address two types of attacks on biometrics: "presentation attacks," which look to use a physical replica of a biometric such as a photo, mask, fake or fake fingerprint to trick a biometric system, and "injection attacks," which look to bypass the camera or biometric sensor completely to inject a fake image into the system. Of the two, it is injection attacks that are used in deepfake attacks – and thus liveness detection technology that can detect and block injection attacks is quickly becoming the more important of the two. The best injection attack solutions confirm three things simultaneously: the user is the right person (matching the ID), a real person (live, not a spoof), and submitting their photo or video right now (proving the authentication is not a replay or deepfake attack).

- 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*

[8] See https://www.dhs.gov/science-and-technology/remote-identity-validation-rally
[9] 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/

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.[10]

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.

Here we note that the emergence of passkeys which enable passwordless logins using the FIDO standards are very promising, and NIST recently issued guidance making clear that passkeys meet Authentication Assurance Level 2 (AAL2) requirements for MFA.[11] 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.

We note that while phishing-resistant MFA is the strongest form of MFA, organizations continue to use a variety of types of MFA to guard against different attacks, including some powered by AI, that seek to compromise the authentication process – in many cases pairing "traditional" MFA (i.e., something you have, know, or are) with the risk analytics tools described in the next bullet.

- Risk analytics engines. These technologies will look at multiple attributes of a user attempting to access a system, such as IP address, device information, geolocation, past user behavior, and other metadata from the user and create a score that the individual is who they claim to be. As with liveness detection, many of the best tools that are being used in risk analytics engines make use of AI themselves. These tools often employ point-in-time assessments at different parts of the identity lifecycle to identify anomalies, deviations, and other risks. Because most of these tools run "behind the scenes," they can be a relatively frictionless way to apply enhanced security measures without degrading the user experience. Real-time account verification and anomaly detection tools have proven effective in identifying fraud vectors such as synthetic identities and Authorized Push Payment (APP) scams, which are increasingly used in

[10] See https://www.ic3.gov/CSA/2022/220418.pdf
[11] See https://pages.nist.gov/800-63-4/sp800-63b.html

conjunction with deepfake typologies. Likewise, real-time verification tools that validate account ownership before transactions are initiated can enhance compliance with AML and KYC frameworks, while also reducing fraud risk in domestic and cross-border payments.

In addition to leveraging predictive tools used in identity proofing, firms have also started to leverage deterministic tools that tie back to authoritative identity sources, such as those run by government.

One example of a deterministic tool is the Social Security Administration's electronic Consent Based Social Security Number Verification (eCBSV) Service, which was launched after Congress directed SSA to do so in 2018; today, financial institutions use it to validate whether someone's name, date of birth, and SSN match the data that is on file in the SSA's systems. This has been a very helpful tool in the fight against synthetic identity fraud, as it is the first time SSA has offered this service through digital channels via an API. At present time, SSA is responding to more than 9 million queries each month.

Beyond helping to stop identity fraud, eCBSV has proven to be a valuable tool to improve financial inclusion – in that many "thin file" applicants for credit who previously might have been flagged by predictive-based fraud engines as being potential synthetic fraudsters now have a clearer path to credit, based on SSA's validation that data submitted corresponds to a real identity. Our members report a 2-4% lift in new credit approvals thanks to eCBSV – proof that better identity solutions offer material benefits to consumers and industry beyond security.

mDLs and other VDCs offer another exciting opportunity to tap into deterministic, authoritative sources of identity. Whereas someone might carry their physical driver's license in their wallet, pocket, or purse, mDLs are typically carried in a "digital wallet," which may be developed by the manufacturer of a smartphone or a third party. In some states, the state itself is the supplier of the digital wallet app.

Moreover the fact that they are built around asymmetric public key cryptography makes them one of the best emerging tools as we seek solutions that can stand up to emerging deepfake attacks.[12] Deepfakes may be able to spoof many biometric tools, but they cannot spoof possession of a private cryptographic key – and so a mDL that relies on public key cryptography can provide a tool for identity proofing/CIP purposes that is not only very secure and privacy-preserving, but also quite easy for consumers to use

[12] We note that use of public key cryptography alone will not blunt every attack, in that ideally, an identity system will verify the correct individual person is actually in control of the device the credential is bound to; if a device falls into the wrong hands, some attacks are possible. The tools used to mitigate identity-related risks for a $500 transaction may differ from the tools used to protect a $500,000 transaction. The strongest verification and authentication solutions will pair cryptography for device and data authentication with biometrics for user authentication.

We believe one idea Treasury should consider is offering grants to states to help to accelerate the launch of privacy-preserving mDLs and other VDCs that can be used to meet CIP purposes across the country. We provide more details here in our response to question 4(d) below.

(a) What factors do financial institutions consider when deciding whether to employ digital identity verification for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use digital identity verification for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use digital identity verification, please provide additional details on the rationale for that decision.

In general, financial institutions that make use of digital identity verification tools for AML/CFT purposes choose to do so based on four factors:

1) How well the tools will help to mitigate risks associated with stolen or spoofed identities
2) The user experience that accompanies use of a tool (since some tools may create so much friction for users that it prompts customers to abandon transactions)
3) The cost of the tool
4) What regulators have said (or might say) about the use of a particular tool or technology

Firms that choose not to use these certain digital identity verification tools generally do so because they fail to satisfactorily address one or more of the above criteria. For example, a solution that can respond to a request twice as fast can be a significant advantage, but that advantage is only meaningful when the output of the request is high quality and reliable. If the a firm's analyst must spend significant time validating or interpreting the information they are getting from a vendor, then any tech efficiency being delivered is effectively nullified. Understanding that balance of needs and organizations requirements is essential to both selecting the right vendor and implementing the right way into an organization.

At a high level, many financial services firms have embraced a strategy relying on APIs and cloud services to facilitate their different screening and due diligence processes. Most of these clients are approaching their API strategies based on clearly defined requirements such as security, response times, throttling, hosting locations coupled with concerns about data quality and operational efficiency. This is especially true for clients with more than 100 million customers.

Going forward, firms are starting to embrace the use of artificial intelligence for CIP purposes. Our members report, however, that many of the newer AI-based solutions in the screening and CIP space overwhelmingly still rely on high quality content curation provided by the handful of major data providers. The effectiveness of these tools requires high quality data that is highly structured, robust, and detailed.

We note that regulatory uncertainty associated with the use of new digital identity verification technologies can often sideline an institution's interest – and believe that a way for Treasury and the prudential regulators to more regularly weigh in on new identity technologies and the permissibility of using these technologies would help to drive innovation in this space.

(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 a general rule, there are no "perfect" digital identity verification tools, in that there is no single tool that will work well for 100% of the population and meet the four criteria listed above. That said, there are most definitely solutions that are better than others – and thus, the threshold for bringing in new technologies to augment or replace existing tools is largely driven by whether they are "materially better" than legacy tools that are in place today.

One theme that runs across the digital identity verification market is that government is the only nationally recognized, authoritative issuer of identity, but the lack of digital counterparts to the physical credentials issued by a mix of Federal, state, and local agencies means that when it comes to online identity verification, the financial services industry is dependent on a marketplace of private sector providers that are trying to essentially guess what, in most cases, only the government truly knows.

This is not to besmirch the capabilities of private providers – there is amazing innovation in this sector, and many of the vendors are quite good at determining if someone is who they claim to be, as well as detecting signs of fraud. However, we believe that going forward, America needs solutions that make greater use of the government's unique role as the authoritative source of identity. Consumers should be able to ask an agency that has already issued them a paper or plastic credential to vouch for them – by validating the information from that credential online. Both eCBSV and mDLs are examples of how these solutions are emerging – but more work is needed to ensure the potential of government digital solutions to reduce illicit finance can be fully realized.

(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.

There are several areas where the financial services sector would benefit from additional insight and guidance from regulators when it comes to using digital identity verification to detect illicit finance and mitigate risks involving digital assets.

One area where our members continue to raise concerns is around the use of new identity verification and authentication technologies – specifically, how regulators will respond to a financial services firm that decides to use them.

We were pleased to see that FDIC recently weighed in with new supervisory guidance on the use of pre-populated information for purposes of meeting Customer Identification Program (CIP) requirements,[13] which helped to clarify that financial institutions are allowed to use these solutions.

Another area where regulatory ambiguities may be inhibiting the adoption of new, more secure identity verification solutions by financial institutions to satisfy CIP requirements is around the use of "mobile Driver's Licenses" (mDLs).

While current CIP guidance makes clear that banks can take a risk-based approach to customer identification – and does not preclude the use of new identification technologies – the new and novel nature of mDLs had led many of our members to report that their compliance teams are not comfortable with using a mDL as part of meeting CIP requirements unless regulators indicate that it is permitted or encouraged. Much of the concern seems to spring from the fact that an examiner may, from time to time, question the use of new and novel tools as being "unproven." With this, our members are concerned about the potential risks involved with a new tool such as a mDL.

From our perspective, regulators should be embracing mDLs:

- They are more secure than plastic driver's licenses, given that they are cryptographically signed by the state government issuers and stored – in most cases – in trusted hardware inside consumer smartphones.
- The REAL ID Modernization Act of 2020[14] specifically recognizes that a mDL can be used to meet REAL ID Act requirements – and the Department of Homeland Security (DHS) has published updated REAL ID regulations outlining the requirements mDLs must implement to be accepted by Federal agencies.[15]
- At a time when identity-related financial fraud and cybercrime is rising (per the FinCEN analysis discussed earlier), mDLs offer a way for consumers to prove who they are for online account opening in a way that is more secure and convenient than many of the legacy solutions used today to support this requirement.
- mDLs can also be better for consumer privacy – in that they allow for a consumer to only choose to share certain data fields from their mDL. A bank should in most cases only need to know the name, date of birth, address, and identification number from

[13] See https://www.fdic.gov/news/financial-institution-letters/2025/fdic-supervisory-approach-regarding-use-pre-populated
[14] See https://www.dhs.gov/archive/real-id/news/2020/12/28/dhs-modernizes-critical-identification-requirements-after-congress-passes-real-id
[15] See https://www.federalregister.gov/documents/2024/10/25/2024-23881/minimum-standards-for-drivers-licenses-and-identification-cards-acceptable-by-federal-agencies-for

a consumer's driver's license, but they should have no need to see a consumer's height or weight, or whether they are an organ donor.

Despite any regulatory uncertainty, banks are very interested in using mDLs. Seven major financial institutions have partnered with the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) on a new project to accelerate the adoption of mDL standards and best practices, and build a reference architecture demonstrating real world business use cases, integrating mDLs with commercially available technology and into business processes including those tied to account opening.[16]

As NIST prepares to publish the outputs of this project later this fall, our members are very eager to see a clear statement from Treasury and the prudential regulators that they are permitted to look to make use of mDLs to meet CIP requirements. Supervisory guidance similar to what FDIC just issued around pre-fill would remove any regulatory ambiguities and put a policy foundation in place for financial services firms to start to adopt more secure, convenient, privacy-preserving identity verification tools in account opening processes.

(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?

As we noted earlier, the Better Identity Coalition has published a Policy Blueprint[17] that outlines a comprehensive 22-point action plan for the U.S. government to take to improve the state of digital identity and authentication – in a way that will help to prevent illicit finance in digital assets, as well as many other related crimes including identity theft and identity-related cybercrime.

A core point we make in the Blueprint is that is the same organized criminals and hostile nation states exploiting the same core weaknesses in digital identity infrastructure to steal billions not just from government – but also banks, healthcare, retailers, fintech services, and cryptocurrency firms.

In other words, this is not just a "digital finance problem," but rather, a national security problem – and thus needs to be addressed not just by Treasury and financial regulators, but with a whole-of-government approach.

More specific to Treasury, we believe there are three steps that Treasury and financial regulators should take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets.

[16] See https://www.nccoe.nist.gov/projects/digital-identities-mdl
[17] See https://www.betteridentity.org/s/Better_Identity_CoalitionBlueprint-January2025.pdf

1) Offer grants to states to help to accelerate the launch of mDLs and other verifiable digital credentials (VDCs) that can be used to meet CIP purposes across the country.

While mDLs and other state-issued VDCs are starting to emerge in states, at present time less than half of states have made such digital credentials available to their residents. Moreover, almost all of the mDLs that have been rolled out today only support in-person identity proofing use cases (i.e., clearing a TSA checkpoint or getting into a bar), whereas the most important use cases with regard to financial services involve those that are for remote (e.g., online) identity proofing.

In our discussions with states, we continually hear two themes:

- First, many states lack the money and resources to move forward with mDLs. State DMVs are generally resource-strapped, and many of them are running their agencies on IT infrastructure that is over 35 years old, based around legacy programing languages like COBOL. While some states have been able to find resources to launch mDL projects, our discussions with DMVs, governors offices, and state legislatures have made clear that getting meaningful deployment across all 50 states is going to take at least 12-15 years if there is not an infusion of resources to accelerate the process.

- Second, states also lack guidance on how to architect remote online identity applications in a way that sets a high bar for security and privacy. This is a concern not only for state governments but also their residents. Indeed, many of the comments already submitted to Treasury on this RFC reflect concerns about the impact that digital identity solutions could have on security, privacy, and civil liberties.

The good news here is that Congress directed NIST to tackle this second issue as part of the CHIPS and Science Act that was passed in 2022. As a result of language included in that law, NIST has launched the "Digital Identities - Mobile Driver's License (mDL)" project at the National Cybersecurity Center of Excellence (NCCoE), focused on creating a "playbook" of standards and best practices that states can follow to ensure that mDLs set a high bar for security and privacy. The project deliverables include specific guidance on how states can architect these tools to preserve and enhance privacy,[18] with a focus on ensuring that mDL solutions cannot be used to track people and allow people to share only a subset of their personal information (vs. traditional driver's licenses today, which by default, share data such as height, weight, organ donor status, and other information that is not relevant to CIP requirements). As noted earlier, NIST has partnered with seven major financial institutions on this project.

[18] See https://pages.nist.gov/nccoe-mdl-project-static-website/pram.html

This ongoing work at NIST provides Treasury and the U.S. government more broadly with a unique opportunity: by offering grant programs to states to accelerate mDL and VDC deployment – with dollars specifically tied to a state's commitment to following this NIST playbook – the government can ensure we realize the benefits of mDL and VDCs more quickly, while also ensuring that states deploying these solutions are doing so in a way that sets a high bar for security, privacy, and the protection of civil liberties. It's a classic example of how the Federal government can offer a "carrot" to states to help ensure that they get digital identity right.

Such a grant program would also provide a critical layer of defense against the rapidly increasing use of deepfakes in illicit finance attacks. Increasingly, deepfakes are being used to spoof voices, photos, and videos, as well to craft sophisticated phishing and impersonation attacks that can more easily dupe consumers. Our members report seeing a sharp increase over the last 18 months in deepfake attacks; attacks that used to be very difficult and resource-intensive to launch are now becoming commoditized, thanks to tools offered by criminal services that have made it cheap and easy for even amateurs to create a convincing deepfake.

As we noted earlier, the fact that mDLs are built around asymmetric public key cryptography makes them one of the best emerging tools as we seek solutions that can stand up to emerging deepfake attacks. Deepfakes may be able to spoof many biometric tools, but they cannot spoof possession of a private cryptographic key – and so a mDL that relies on public key cryptography can provide a tool for identity proofing/CIP purposes that is not only very secure and privacy-preserving, but also quite easy for consumers to use.

2) **Make clear that portable digital identity credentialing tools that have been certified as meeting IAL2 requirements (as defined in NIST's 2025 revision of its Digital Identity Guidelines, SP 800-63A-4)[19] can be used to fulfill CIP requirements.**

While we are enthusiastic about the role that government-issued mDLs and other VDCs can play in addressing illicit finance challenges, we also realize 1) that getting to critical mass with these credentials will take years, and 2) some Americans may not want to use a government-issued digital credential.

One way that Treasury can address these concerns is to affirmatively state that financial services firms may choose to rely on accredited private-sector credential service providers (CSPs) that have been certified as meeting the latest version of IAL2 requirements.

[19] See NIST SP 800-63A-4, Digital Identity Guidelines - Identity Proofing and Enrollment at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.pdf

We note up front that some of our members have been skeptical about the value of current IAL2-certified solutions (tied to the prior version of NIST's Digital Identity Guidelines, SP 800-63-3), in that the certification process did not test the effectiveness of the solutions; instead it focused solely on the processes use to meet the NIST requirements. As a result, a financial services firm looking at six different IAL2-certified solutions would likely see six very different levels of performance.

The newest NIST guidance, however, took significant steps to address this concern: as part of being IAL2-certified under SP 800-63A-4, a CSP must ensure (per sections 3.11 and 3.13 of the NIST guidance) that the products it uses for both remote document authentication and the 1:1 biometric verification to the photo on that identity document (i.e., "selfie match" tools) have been tested by independent entities (such as accredited laboratories or research institutions) to demonstrate that they can perform at a high level across demographic groups. With this new mandate for testing, we believe that CSPs that demonstrate their ability to meet IAL2 requirements under SP 800-63A-4 should be able to be trusted as one option for financial service firms to address CIP requirements.

Such a change would help to address a few issues:

- It would create a new option for Americans to prove their identity for CIP purposes using a credential they already have, rather than starting from scratch.
- It would create another option for Americans to prove their identity for CIP purposes without having to rely on a government-issued digital credential.
- It would demonstrate that Treasury is embracing private sector innovation in digital identity – while doing so in a way that also sets a meaningful floor to address security and illicit finance concerns.

3) **Look more broadly beyond financial services firms to other firms that also play a role in the "fraud and scam ecosystem."**

While financial services firms have significant responsibility in guarding against illicit activity, they are increasingly dealing with an ecosystem where attackers are leveraging companies outside of the financial services sector to launch attacks. The volume of fraud and scams that originate through text message or on social media is significant. Per the Federal Trade Commission (FTC):

- Consumers reported losing $470 million to scams that started with text messages in 2024 – an amount that is five times higher than what was reported in 2020.[20]

- Consumers reported losing $2.7 billion to social media scams since 2021 – more than any other contact method.[21]

- Investment scams – many of which focus on crypto – led to losses of $5.7 billion in 2024, per the FTC. Impostor scams led to another $2.95 billion lost. And per the FTC, "in 2024, consumers reported losing more money to scams where they paid with bank transfers or cryptocurrency than all other payment methods combined." [22]

It will be very difficult to truly reduce illicit finance in the digital assets space if efforts to combat illicit finance activities are focused solely on the financial services sector. This is a bigger problem and solutions must look across the ecosystem.

(e) Treasury will evaluate digital identity verification and consider its impact based on the research factors identified in the GENIUS Act. Provide any information pertinent to those factors.

Per the GENIUS Act, seven research factors will guide Treasury's research into "innovative or novel methods, techniques, or strategies that regulated financial institutions use, or have the potential to use, to detect illicit activity, such as money laundering, involving digital assets." These factors include:

1) Improvements in the ability of financial institutions to detect illicit activity involving digital assets.
2) Costs to regulated financial institutions.
3) The amount and sensitivity of information that is collected or reviewed.
4) Privacy risks associated with the information that is collected or reviewed.
5) Operational challenges and efficiency considerations.
6) Cybersecurity risks.
7) Effectiveness of methods, techniques, or strategies at mitigating illicit finance.

As we noted earlier, we believe there are four core factors that financial services firms look at when it comes to that make use of digital identity verification tools. We note that two of them are not reflected in the criteria above:

[20] See https://www.ftc.gov/news-events/news/press-releases/2025/04/new-ftc-data-show-top-text-message-scams-2024-overall-losses-text-scams-hit-470-million
[21] See https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-data-shows-consumers-report-losing-27-billion-social-media-scams-2021
[22] See https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

- The user experience that accompanies use of a tool (since some tools may create so much friction for users that it prompts customers to abandon transactions)
- What regulators have said (or might say) about the use of a particular tool or technology

We believe it would make sense for Treasury to also consider these factors in its research.

Beyond looking at these factors, we also believe more research is needed to quantify the impact of illicit finance. Earlier, we discussed the valuable work that FinCEN has launched in quantifying the percentage and dollar value of SARs that are tied to a compromise of identity. We believe FinCEN should continue its work here, and would suggest that FinCEN should publish an annual report that analyzes SARs from the previous year – with a focus on incidents that are tied to a compromise of identity – and details what has changed.

We greatly appreciate the willingness of the Treasury Department to consider our comments and suggestions, and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at jeremy.grant@venable.com.