BETTER IDENTITY COALITION, JEREMY GRANT

Proposal and Comment Information

Title: Permitted Payment Stablecoin Issuer Customer Identification Program, R-1885

Comment ID: FR-2026-0005-01-C14

Subject

Comments on R-1885 and RIN 7100-AH1 - Proposed Rule for Permitted Payment Stablecoin Issuer Customer Identification Program.

Submitter Information

Organization Name: Better Identity Coalition

Organization Type: Organization

Name: Jeremy Grant

Submitted Date: 08/21/2026

NONCONFIDENTIAL // EXTERNAL

The Better Identity Coalition appreciates the opportunity to provide input to the government on the Proposed Rule for Permitted Payment Stablecoin Issuer Customer Identification Program.

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, health care, technology, fintech, payments, and security.

Our comments are attached. We greatly appreciate the willingness of the Federal Reserve 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<mailto:jeremy.grant@venable.com>.

Jeremy A. Grant
Managing Director, Technology Business Strategy | Venable LLP
Coordinator | Better Identity Coalition

t 202.344.4646 | m
600 Massachusetts Avenue, NW, Washington, DC 20001

Comments to the Financial Crimes Enforcement Network, Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and National Credit Union Administration

Proposed Rule - Permitted Payment Stablecoin Issuer Customer Identification Program

August 2026

The Better Identity Coalition appreciates the opportunity to provide input to the government on the *Proposed Rule for Permitted Payment Stablecoin Issuer Customer Identification Program.*

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, health care, technology, fintech, payments, and security.

Up front, we note that of our 20 members, roughly half are either financial institutions, fintech, 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 and FinCEN's recent work around digital identity – including highlighting the importance of digital identity in this proposed rule and pledging in March 2026 report to Congress on "Innovative Technologies to Counter Illicit Finance Involving Digital Assets" to issue guidance to financial institutions on how they can utilize verifiable digital credentials consistent with their existing customer identification programs.

With regard to this proposed rule, we are pleased to see that the draft discusses digital identity, with a focus on emerging technologies and tools in this space that can help to drive material improvements in Customer Identification Program (CIP) outcomes. A significant portion of illicit activity in digital assets (and financial services more broadly) is tied to compromises of identity or authentication – and the government has a significant role to play in:

1) Updating regulations to make clear to regulated entities that they can use the most promising emerging technologies and tools in digital identity, and

2) 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. The Financial Services Sector Coordinating Council (FSSCC) tackled this issue earlier this year as part of the guidance it crafted in partnership with the Finance and Banking Information Infrastructure Committee (FBIIC), as part of the AI Executive Oversight Group (AIEOG) established by Treasury.[7] Through this initiative, two papers were published:

- *Mitigating AI-Powered Attacks Against Identity and Authentication* identifies the top ten attack vectors that financial institutions face because of Gen AI, and details specific tools

[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
[7] See https://home.treasury.gov/news/press-releases/sb0395

those institutions can use to detect and stop those attacks. The paper also includes a new Maturity Model for Identity Controls to Combat Gen AI-powered Attacks – recognizing that resource constraints in smaller institutions pose challenges that may be easier to solve for larger ones – and laying out steps that institutions at every level of sophistication can take to get started.

- *Recommendations for Policymakers: Mitigating AI-Powered Attacks Against Identity* and *Authentication* is a companion piece that outlines the role that government needs to play to help address these attacks – outlining 20 distinct actions for policymakers and regulators.

Many of the recommendations we offer in response to this proposed rule are drawn from the second paper.

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 Section VI of the RFC.

5. **Should the regulatory text explicitly discuss digital identity solutions or verifiable credentials? How could it best do so given the range of tools available on the market?**

   We believe what is needed most is clear guidance on how government-issued verifiable digital credentials (VDCs) such as mobile driver's licenses (mDLs) can be used across the financial services industry. This is an issue that is highly relevant to stablecoins, but guidance should not be specific to stablecoins.

   In that regard, while it might be helpful to include such guidance as this rule is finalized, what would be most helpful is guidance in line with what Treasury pledged to issue in the March 2026 report to Congress: guidance to financial institutions on how they can utilize verifiable digital credentials consistent with their existing customer identification programs.. That could then be referenced in these final regs and/or restated in the final text.

   As the proposed rule states, "the proposed rule would subject PPSIs to CIP requirements that are comparable to existing CIP requirements for other financial institutions, such as banks, broker-dealers, mutual funds, and FCMs and IBCs." Given this we believe what is most important is clear and consistent guidance on how an emerging class of verifiable digital credentials can be used across all of these institutions.

   In terms of the different types of digital credentials that are available, we believe it is best to break them down into two categories:

   a) Government-issued VDCs. In addition to mDLs and other government-issued VDCs such as digital birth certificates and Social Security number cards, this category also includes credentials that are securely derived from a credential such as a passport where creation

of the credential in a digital wallet is tied to cryptographic validation of the security chip in the physical credential.

b) Privately issued VDCs that have been certified as meeting NIST Identity Assurance Level 2 (IAL2) requirements (as defined in NIST's 2025 revision of its Digital Identity Guidelines, SP 800-63A-4).

mDLs and other government-issued VDCs offer an exciting opportunity for financial services firms to leverage 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.[8] 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.

At the moment, our members believe that 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.

[8] 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.

- The REAL ID Modernization Act of 2020[9] 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.[10]
- 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 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. Eight 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.[11]

Now that NIST has published the initial public draft that contains the outputs of this project as SP 1800-42, "Digital Identities – Mobile Driver's License (mDL): Accelerating Development and Adoption of Digital Identity for Financial Institutions,"[12] 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 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.

With regard to privately issued VDCs, we believe guidance should 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)[13] can be used to fulfill CIP requirements.

[9] See https://www.dhs.gov/archive/real-id/news/2020/12/28/dhs-modernizes-critical-identification-requirements-after-congress-passes-real-id
[10] See https://www.federalregister.gov/documents/2024/10/25/2024-23881/minimum-standards-for-drivers-licenses-and-identification-cards-acceptable-by-federal-agencies-for
[11] See https://www.nccoe.nist.gov/projects/digital-identities-mdl
[12] See https://csrc.nist.gov/pubs/sp/1800/42/ipd
[13] 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

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 regulators 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.

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 regulators are 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.

6. What are the benefits and risks of using digital identity solutions or verifiable credentials as part of verifying customers' identities?

Broadly speaking, digital identity solutions are used today to support every digital account opening. The primary question from a regulatory perspective is whether regulators are making clear that newer tools that are more effective than legacy tools are permitted to be used.

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 – we just made the case in our answer to question 5 that regulators should make clear that portable digital identity credentialing tools that have been certified as meeting IAL2 requirements can be used to address CIP requirements. 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 – allowing financial services firms to rely more on deterministic identity tools alongside, or instead if, the predictive tools that are most commonly used today.

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 mDLs and the Social Security Administration's electronic Consent-Based SSN Verification System (eCBSV) 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.

We are also hearing from our members of an increasing need to use mDLs and other VDCs for in-branch CIP, as the widespread availability of deepfake technology is making it easier than ever to create fake physical IDs that criminals then use to open accounts in other people's names.

With regard to risks, we believe the benefits here far outweigh the risks – but where there are risks, following NIST's new guidance on mDLs for the financial services sector is the best way to address them. SP 1800-42 outlines a threat model and privacy considerations, and provides concrete guidance on how to address them – ensuring that as mDLs and other

government VDCs are used, they maximize privacy and security benefits and minimize potential risks.

7. **What is the expected likelihood that a PPSI would rely on another PPSI's CIP or the CIP of another Federal functionally regulated financial institution's CIP?**

   While the reliance clause has been in place for more than 20 years, it is very rarely used today. Our members believe this is due to a number of factors, including the complexities involved with setting up reliance agreements, concern that regulators may raise concerns about these agreements and the decision to rely on another institution's CIP processes, and an overall lack of strong business reasons to do so.

   That said, our general observation is that newer companies in the financial services space, such as fintechs and cryptocurrency firms, are more likely to be interested in leveraging the reliance clause than legacy banks.

   On that note, Permitted Payment Stablecoin Issuers (PPSI) are likely to encompass a variety of entities, from large banks in traditional finance to startups. We expect that some of the newer entrants will be more willing to explore reliance – but note that as with mDLs and other VDCs, additional guidance on use of reliance clause would be helpful, and could open up the number of firms willing to rely on CIP processes carried out by other institutions.

We greatly appreciate the willingness of FinCEN, OCC, FDIC, the Federal Reserve, and NCUA 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.