OpenID Foundation
2603 Camino Ramon, Suite 200
San Ramon, CA 94583

Honorable Scott Bessent
Acting Director
Consumer Finance Protection Bureau
1700 G St NW
Washington, DC 20552

October 17, 2025

Dear Director Bessent

Thank you for the opportunity to comment on the Treasury's Request for Comment on **TREAS-DO-2025-0070-0001 "**Innovative Methods To Detect Illicit Activity Involving Digital Assets," in line with the GENIUS Act and Executive Order 14178 on ''Strengthening American Leadership in Digital Financial Technology.'' Exhibit A is a summary of recommendations and Exhibit B elaborates on the questions raised by the Treasury Department for comment.

By way of background, the OpenID Foundation (OIDF) is a non-profit, technical standards organization whose mission is to lead the global community in creating open, identity standards that are secure, interoperable, and privacy-preserving. Founded in 2007, our standards are selected by the the private and public sector alike and deployed by millions of developers ranging from startups to the largest digital platforms and governments.

The US government regularly selects our specifications to protect US critical infrastructure, and we work in close collaboration with NIST on efforts like on their SP 800-63-4 Digital Identity Guidelines and NIST NCCoE Mobile Driving License project. OIDF specifications are widely recognized by government and public sector implementers including OpenID Connect (3+ billion users daily globally for login, single sign on), FAPI used in billions of open banking and open data transactions, and OpenID for Verifiable Presentation and Verifiable Credential Issuance (37 countries selected these specifications for digital wallet deployments), and Shared Signals for real time risk exchange across ecosystems (recommended by US CISA). Our standards such as OpenID Connect have also been recognized by ISO and ITU-T as standards recognized by them as treaty-based standards bodies. Today, the OpenID Foundation's standards are the connective tissue to enable people to assert their identity and access their data at scale, the scale of the internet, enabling "networks of networks" to interoperate globally. Find out more at openid.net.

Our standards are essential for safeguarding the financial ecosystem. They play a critical role in preventing bad actors from gaining access to financial institutions, or the broader US financial system … and if they do, to enable participants across the ecosystem to share risk signals effectively. These standards apply equally to traditional finance and digital assets, as well as to other sectors such as healthcare, insurance, government services, cloud computing.. They deliver security, interoperability, scalability, and consent-based privacy-preserving release of user data. All our standards are developed in alignment withWTO best practices for standards development. We go further by subjecting our specifications to rigorous mathematical security analysis before they advance to Final status. Of our many standards, the ones we believe are most relevant to the objectives of the Genius Act and this request for comments are as follows:

- **OpenID for Verifiable Credential Issuance, OpenID For Verifiable Presentation, the High Assurance Interoperability Profile**: Standards for verifiable credentials which have been adopted by 37 countries, and they are in active use by 1.3M Americans already.
- **OpenID Connect and FAPI 2.0:** Standards for the secure data exchange of information between and within entities.
- **OpenID Federation**: Universal trust discovery and management protocol for different ecosystems (federated and verifiable credential-based).
- **OpenID for Identity Assurance**, used to exchange assurance information between parties such as NIST SP 800-63-4 Digital Identity Guidelines and the risk based levels of assurance defined by them.
- **Shared Signals Framework, CAEP, RISC:** Standards for the sharing of signals amongst ecosystem participants, within and across organizations, public and private

Any effort to enable the safe and secure scaling of digital asset infrastructure can and should include use of OIDF specifications, open source tests, and conformance tools.

Our standards are not designed for racking or identifying illicit activities (such as those occurring on a blockchain). While that is important work, it focuses on pursuing criminal activity after it has already happened.. Our approach addresses the root causes of financial cybercrime - preventing bad actors from committing a crime in the first place.

OIDF supports the GENIUS Act's dual objectives of law-enforcement capability and privacy preservation. Partially anonymous, partially unlinkable authentication under ISO/IEC 29191 achieves both: it prevents routine PII exposure while allowing a designated opener (such as FinCEN or authorized law-enforcement bodies) to re-identify claimants under due process. This technical balance aligns with the GENIUS Act's mandate for responsible innovation in digital finance.

We hope these comments are material and useful in your deliberations. We welcome further discussion on our comments, and you can reach us directly at director@oidf.org to organize a discussion.

Sincerely,

Gail Hodges
Executive Director
OpenID Foundation

Exhibit A - Summary of Recommendations

Research Factors on Relevant APIs:

Research Factor (Expected Statutory Focus)	Information Pertinent to the Factor (Impact of OIDF API Standards)
1. Security and Fraud Mitigation	**OpenID FAPI 2.0 & Shared Signals Framework (SSF) APIs** deliver a unified, high-assurance security standard. FAPI 2.0 is selected globally for open banking and open data to rationalize porous SaaS architecture. Impact: These APIs reduce cybercrime exposure by standardizing security profiles across the stablecoin ecosystem and enabling Permitted Payment Stablecoin Issuers to exchange real-time risk intelligence (SSF), which is crucial for mitigating account takeover and synthetic identity fraud before it affects assets regulated by the GENIUS Act.
2. Interoperability and Scalability	**OpenID for Verifiable Credential (VC) Issuance & Presentation APIs** are the connective tissue for a "network of networks." They are utilized by 37 countries for digital wallet deployments. **Impact**: This global scale and proven interoperability is essential for the future of digital assets. By adopting OIDF standards, the U.S. ensures that **Permitted Payment Stablecoin Issuers** are not limited to a closed, domestic-only system, but can achieve global scale and align with international standards like FATF Digital ID Guidance and EU eIDAS 2.0, supporting the global leadership objective of the GENIUS Act.
3. Efficiency and Cost Reduction	**Verifiable Credential (VC) API-based Verification** is the lowest-cost, highest-assurance method for Customer Identification Program (CIP) compliance. **Impact:** For the new Permitted Payment Stablecoin Issuers facing new BSA/AML mandates, VCs eliminate the high per-check cost of traditional data bureaus and manual document review. Treasury's sanctioning of VC APIs facilitates effective, risk-based adoption by making high-integrity identity verification economically viable for all market participants, fostering the national innovation championed by the GENIUS Act.
4. Privacy and Data Minimization	**Verifiable Credential and Privacy-Enhancing Technology (PET) APIs** enable attribute-based verification (e.g., proving "over 21" or "US Person" without sharing the full date of birth or address). **Impact:** These APIs directly implement the principle of data minimization, allowing **Permitted Payment Stablecoin Issuers** to comply with CIP/AML laws without over-collecting and warehousing unnecessary Personally Identifiable Information (PII). This reduces the issuer's data breach liability and fosters consumer trust in the regulated stablecoin products established by the **GENIUS Act.**

Steps the U.S. Government Should Take	Rationale and Linkage to the GENIUS Act (The Improvement)
1. Explicitly Sanction Verifiable Digital Credentials (VDCs) as "Documentary Evidence" for CIP Compliance. Action: Treasury/FinCEN must issue immediate, unambiguous guidance clarifying that VDCs—issued by trusted authorities and utilizing approved technical standards (e.g., OIDF's OpenID for VC and NIST SP 800-63-4 IAL2)—constitute **"documentary evidence"** for CIP requirements.	**GENIUS Act Link:** This step directly addresses the primary regulatory obstacle for **Permitted Payment Stablecoin Issuers** under **Section 4(5)(A)(v)**, which subjects them to new BSA/AML obligations. Without this clarity, these new entities cannot effectively leverage API-driven identity solutions, forcing them to rely on outdated, high-cost, and less secure manual processes. This is the foundation for effective, risk-based API adoption.
2. Mandate the Use of High-Assurance API Security Standards. Action: Federal regulators (Primary Federal Payment Stablecoin Regulators) should require that all APIs used by **Permitted Payment Stablecoin Issuers** for transmitting sensitive customer data, account information, or financial transaction commands conform to a recognized high-security standard, such as **FAPI 2.0** (Financial-grade API Security Profile).	**GENIUS Act Link:** The security of the payment stablecoin ecosystem is paramount. Requiring **FAPI 2.0** establishes a single, non-negotiable security baseline for the data flow *between* regulated entities. This facilitates **risk-based adoption** by ensuring API integrations are uniformly secure, reducing the collective systemic risk and protecting customers who hold payment stablecoins issued under the Act.
3. Establish a National Standard for Real-Time Risk Signal Exchange. Action: The U.S. government should formally recognize and promote an open standard, such as the **OpenID Shared Signals Framework (SSF),** as the preferred or mandatory API specification for real-time risk intelligence sharing (e.g., account takeover and anti-fraud alerts) among **Permitted Payment Stablecoin Issuers** and other financial institutions.	**GENIUS Act Link:** APIs are essential for detecting illicit finance *in real-time*. This step enables the new stablecoin regulatory class to move beyond reactive SAR filing to **proactive mitigation**. The standardization of risk communication through OIDF's SSF will allow **Permitted Payment Stablecoin Issuers** to interoperate seamlessly with the broader financial sector, bolstering the integrity of the U.S. financial system that the **GENIUS Act** seeks to strengthen.

4. Fund Interoperability and Pilot Programs for Compliant APIs. Action: Congress and Treasury should fund programs, potentially leveraging the NIST NCCoE, specifically tasked with creating and sharing open-source reference architecture and API implementations that demonstrate how **Permitted Payment Stablecoin Issuers** can meet their CIP/KYC and Travel Rule obligations using open identity and security standards.	**GENIUS Act Link:** Adoption of innovative APIs is hindered by the high initial cost of proof-of-concept and legal review. Government-funded reference implementations and pilot projects—focused on the new compliance requirements of the **GENIUS Act**—would drastically reduce the operational barrier to entry, accelerating the safe and risk-based adoption of compliant API technologies across the entire stablecoin market.
5. Recognize Partially Anonymous, Partially Unlinkable Authentication as Permitted under GENIUS Act Section 4(5)(A)	Action: FinCEN should issue interpretive guidance clarifying that digital-identity frameworks based on OpenID Connect and OpenID Federation with ephemeral subject identifiers qualify as acceptable privacy-enhancing authentication mechanisms under CIP/KYC obligations, so long as they retain a designated re-identification path for law-enforcement access. This guidance would implement ISO/IEC 29191 requirements and support risk-based adoption of API-enabled privacy controls envisioned by the GENIUS Act.

Recommendations to Unblock Obstacles

Obstacle (Issue Identified)	Recommendation (Proposed Solution)	GENIUS Act Linkage (The Improvement)
1. Regulatory/ Supervisory Ambiguity in CIP/KYC	**Recommendation 1.1 (API-Enabling Guidance):** Treasury/FinCEN should issue guidance that explicitly recognizes **Verifiable Digital Credentials (VDCs)** that meet standards (e.g., NIST SP 800-63-4 IAL2, OIDF profiles) as constituting "**documentary evidence**" for CIP purposes.	This is the single largest barrier to the scaled, low-cost compliance needed for the new class of **Permitted Payment Stablecoin Issuers** under **Section 4(5)(A)(v) of the GENIUS Act**. Clarifying VDCs as documentary evidence will unlock the use of API-based identity proofing and enable stablecoin issuers to meet their new BSA/AML mandates efficiently.

2. Operational Siloing in Risk Mitigation	**Recommendation 2.1 (Standardized Risk APIs):** Mandate or strongly incentivize the use of API standards, such as the **OpenID Shared Signals Framework (SSF)**, for the real-time, standardized exchange of risk signals (e.g., account takeover, PII compromise) between regulated entities.	The **GENIUS Act** introduces a new, interconnected stablecoin ecosystem. Relying solely on internal, legacy systems is an operational obstacle. APIs using the SSF standard are the fastest, most effective way for **Permitted Payment Stablecoin Issuers** and other FIs to share the real-time intelligence necessary to mitigate fraud related to stablecoin accounts.
3. Legislative Inertia in the Travel Rule	**Recommendation 3.1 (Travel Rule Modernization):** The Travel Rule (31 CFR § 1010.410(f)) must be updated to explicitly permit compliance via API-based, privacy-enhancing methods, allowing the transfer of cryptographically verifiable proof of required originator/beneficiary information instead of unencrypted PII.	The current Travel Rule creates a legislative obstacle for API-driven, privacy-preserving digital asset transfers. Modernizing this rule will allow **Permitted Payment Stablecoin Issuers** to achieve full compliance with data-sharing requirements under **Section 4(5)(A)** while simultaneously upholding the principle of data minimization, which is vital for building public trust in regulated digital assets.
4. Lack of a Common API Security Baseline	**Recommendation 4.1 (Mandate High-Assurance API Standards):** Federal supervisors should require the use of high-assurance security profiles—such as **FAPI 2.0**—for all APIs used by **Permitted Payment Stablecoin Issuers** and their third-party identity partners to secure the movement of customer data.	The complexity of digital asset services increases the attack surface. **FAPI 2.0** provides a common, high-security baseline for financial APIs. Mandating its use will remove the operational obstacle of disparate security controls, ensuring that the new regulatory landscape introduced by the **GENIUS Act** is built upon a resilient and standardized security foundation, consistent with OIDF's reference architectures.
5. Absence of Legal Recognition for Partially Anonymous Authentication Current AML regulations lack clear provisions for controlled anonymity and unlinkability required for privacy-	**Recommendation 5.1:** Treasury should amend 31 CFR § 1020.220 to explicitly permit authentication models compliant with ISO/IEC 29191 where a designated opener can re-identify claimants under lawful process. This balances law-enforcement visibility with the **GENIUS Act's** goal of privacy-preserving innovation.	

preserving compliance.		

Additional Considerations	Reasoning and Impact
1. CONSIDER recognizing verifiable digital credentials (VDCs) issued by many acceptable sources as valid evidence under Customer Identification Program (CIP) and Customer Due Diligence (CDD) obligations, including as “documentary” verification methods when appropriate specifically for compliance with the GENIUS Act. Treasury and FinCEN could interpret 31 CFR § 1020.220 (and corresponding CIP rules and guidance) to include verifiable digital credentials if they can meet industry standards, such as a baseline of National Institute of Standards and Technology (NIST) SP 800-63-4 Identity Assurance Level 2 (IAL2) identity verification or higher, issued directly from government authorities, or through reliance upon approved institutions or identity trusts.**Crucially, these VDCs should be treated as "documentary" evidence to enable Permitted Payment Stablecoin Issuers to effectively and**	OIDF elaborates on how OpenID For Verifiable Credentials can be leveraged to comply with CIP/KYC regulations and financial institution current best practices and processes in the attached documents: ● **OpenID 4 Identity Assurance KYC Metadata requirements** ● **OIDF Extended eKYC considerations** The longstanding reliance on physical IDs shapes the perspectives of regulators and compliance officers, many of whom are unfamiliar with how digital identity credentials and the secure methods by which they are issued and managed provide high assurance identity verification and authentication strengthening legal compliance by default. Current CIP programs largely assume the use of physical IDs, even though the statute does not mandate any specific medium or security mechanism. Verifiable digital credentials issued by trusted authorities offer cryptographically proven authenticity and stronger protection against forgery or impersonation, better supporting the objectives of risk-based compliance programs. Recognizing VDCs as documentary evidence is a necessary modernization step that will directly support the objectives of the GENIUS Act by enhancing verification accuracy, reducing compliance costs for new Permitted Payment Stablecoin Issuers, and aligning

efficiently comply with their new Customer Identification Program (CIP) and verification requirements under Section 4(5)(A)(v) of the GENIUS Act, which newly classifies them as financial institutions for Bank Secrecy Act (BSA) purposes. These verifiable digital credentials (VDCs) could be treated as “documentary” evidence where appropriate. The principle of data minimization should become a pillar of financial compliance, enabling VDC-enabled attribute verification encouraged over requiring the sharing of unnecessary personally identifiable information (PII), such as static identity documents, where possible.	U.S. practice with FATF Digital ID Guidance (2023) and EU eIDAS 2.0, promoting global interoperability. To date, 37 jurisdictions globally are issuing or planning to issue verifiable credentials using the OpenID for Verifiable Credentials specifications. To remain competitive and interoperable, the US will want to seriously consider strategies that support state issuance and FI acceptance, along with acceptance by the USG and in other industry verticals. Attribute-based approaches to AML, could also be explored like “not-on-sanctions-list” or “US-person,” to manage risks without the overcollection of PII data. For avoidance of doubt, the use of VDCs does not negate or replace the need for federated protocols like OpenID Connect and FAPI 2.0. These will always have their place as well, especially during the identification process.
2. Permit Permitted Payment Stablecoin Issuers to rely on verifiable digital credentials (VDCs) issued by other regulated entities, identity trusts, or accredited sources via verified real-time APIs for AML/CFT compliance. Treasury and FinCEN may want to authorize Permitted Payment Stablecoin Issuers to accept credentials and attestations from peer financial institutions or identity trust networks when those issuers meet assurance and audit standards. Providing regulatory clarity for Permitted Payment Stablecoin Issuers to rely on third-party identity proofing solutions is crucial for their new operations and accelerates the safe onboarding of customers holding or using stablecoins, which are a central focus of the GENIUS Act. Congress should further consider the addition of a new § 201(d) to the *Digital*	In the US, issuance of verifiable credentials is currently state led, as seen with the 18 states issuing mobile driving licenses, enabling millions of Americans with mDLs for daily use. In this context, US states and jurisdictions are “other regulated entities” that would be logical to permit for use in verified real-time APIs for AML/CFT compliance. Other sources of accredited sources and identity trusts exist outside the US and are started to emerge in the US too. In other jurisdictions, bank consortia (BankID in Sweden, BankID in Norway, ConnectID in Australia, and SelectID in UK) are offering identity services in standardized ways permitted under local laws. Such services may also emerge in the US market. The US Government is likely going to want to be open to innovation and support both state issued and private sector issued credentials. This is happening today in the US with "derived" passport credentials. TSA/DHS accept both state issued mDLs for travel through TSA checkpoints, and Google and Apple "derived" passport credentials. These are credentials derived using scans of real passports but then a new digital identity credential is created and signed by Apple and Google (not by the US State Department) and stored in Apple Wallet and Google wallet respectively. With appropriate safeguards, private sector issued credentials can help accelerate market adoption and

Asset Market Structure Discussion Draft (Sept. 2025) clarifying Treasury's authority to recognize and accredit digital-identity and privacy-enhancing compliance frameworks.	serve a wide range of identity use cases at a pace that state entities and federal entities are not well equipped to support. Specifically for the GENIUS Act, statutory clarity ensuring Permitted Payment Stablecoin Issuers can rely on third-party verification is essential for scalable compliance. While current CIP programs still assume physical ID presentation, the underlying statute is technology neutral and does not mandate any specific medium or security mechanism. Recognizing and adopting VDCs can transform onboarding by reducing costs and friction, improving AML data quality and transparency, and enabling faster, more collaborative investigations across institutions and borders—all while minimizing data-collection risk. Global identity ecosystems are interconnected, and weaknesses in one jurisdiction can quickly cascade across borders. Fragmented standards create exploitable gaps for synthetic identities and other forms of fraud. International harmonization is essential to align assurance policies across platforms and jurisdictions, enable cryptographic binding of identity constructs through interoperable frameworks, reduce regulatory arbitrage by converging AML/KYC requirements with FATF and FinCEN guidance, and facilitate real-time intelligence sharing. Without such coordination, identity assurance remains fragmented, leaving financial systems vulnerable to systemic exploitation on a global scale. Statutory clarity ensures that Treasury's modernization efforts rest on a durable, technology-neutral foundation. This amendment would future-proof the U.S. AML/CFT regime, align it with G7 digital-identity roadmaps, and strengthen U.S. leadership in global digital-asset regulation. OIDF standards such as OpenID Connect with ephemeral subject identifiers and OpenID Federation Trust Frameworks already meet Unlinkability Level UL 3+ (RP–User, AP–RP, Active Outsider–User, Passive Outsider–User) as demonstrated in Annex C of ISO/IEC 28551. Combining these mechanisms with an authorized designated opener satisfies the ISO/IEC 29191 requirement for controlled re-identification, allowing Permitted Payment Stablecoin Issuers to authenticate users securely while ensuring law-enforcement traceability. OIDF as a Co-Organizer of SIDI Hub is working to map trust frameworks across jurisdictions, bringing depth to the OECD Digital Identity Recommendations, FATF Digital identity guidelines, UNDP Digital Identity Safeguards, and World Bank client support. When mature, this trust framework mapping has material potential to

	underpin not only financial services use cases, but a broad spectrum of cross border interoperability requirements and use cases. By applying AI tooling, SIDI Hub is working at pace to accelerate delivery and validate country-by-country maps with government officials like NIST, Australian Data Standards Body, Canadian DIACC, Kenyan government and others. http://Sidi-hub.community
3. Permit privacy-enhancing technologies (PETs) to meet verification and monitoring obligations. Treasury and FinCEN should explicitly recognize and permit the use of PETs to fulfill the Customer Identification Program (CIP) and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) obligations newly imposed on Permitted Payment Stablecoin Issuers under Section 4(5)(A) of the GENIUS Act.	PETs enable institutions to prove AML/CFT compliance without exposing underlying PII, minimizing data-breach and insider-risk exposure while maintaining verifiable oversight. Recognizing PETs would modernize compliance architecture for new stablecoin issuers, lower data-handling costs, and encourage innovation consistent with global privacy and financial-integrity standards, while allowing them to meet the stringent BSA requirements of the GENIUS Act. Treasury and FinCEN should explicitly recognize authentication architectures compliant with ISO/IEC 29191 *Partially Anonymous, Partially Unlinkable Entity Authentication* as qualifying Privacy-Enhancing Technologies under Section 4(5)(A) of the GENIUS Act. Such architectures can be realized through global open standards OpenID Connect and OpenID Federation using ephemeral subject identifiers or Self-Issued OpenID Providers (SIOP). These mechanisms enable verifiers to authenticate a claimant without receiving persistent identifiers, ensuring that each transaction remains unlinkable while preserving a re-identification path for a designated opener such as FinCEN, consistent with ISO/IEC 29191 Clauses 5 a)–c).

4. Modernize the Travel Rule to enable verifiable digital credential-based information transfer. Treasury could amend 31 CFR § 1010.410(f) or issue guidance allowing originator/beneficiary data, , which must now be collected by Permitted Payment Stablecoin Issuers under Section 4(5)(A) of the GENIUS Act, to be transmitted via cryptographically verifiable credentials or proofs instead of plaintext PII.	The current Travel Rule framework was built for wire transfers, not blockchain systems. For transactions involving payment stablecoins regulated under the GENIUS Act,verifiable digital credentials can carry or attest to required information with integrity, selective disclosure, and traceability. This approach preserves law-enforcement visibility while protecting privacy, ensuring interoperability with FATF Recommendation 16.
5. Leverage NIST NCCoE collaboration for technical pilots and standards. Treasury and FinCEN should partner with NIST's National Cybersecurity Center of Excellence to pilot mobile driver's licenses (mDLs), VDCs, and interoperable trust registries for CIP and KYC testing. This collaboration should prioritize creating a technical roadmap for the deployment of OIDF standards by Permitted Payment Stablecoin Issuers to achieve compliance with Section 4(5)(A) of the GENIUS Act.	The NCCoE provides a vendor-neutral, collaborative environment where industry, government and academia work together to address identity assurance challenges. Through this community-driven approach, NCCoE develops standards-based prototypes such as, NIST SP 800-63-4 and ISO 18013-5 for mobile drivers license (mDL), along with 18013-7 for online presentation - that demonstrate real-world feasibility and assurance equivalence. Collaboration ensures technical soundness, interagency alignment, and rapid deployment of privacy-preserving digital-identity frameworks.
6. Direct FinCEN to engage proactively with industry on adoption of advanced technologies that enhance AML compliance, investigations, and privacy protection. Treasury could issue formal direction or guidance requiring FinCEN to establish an ongoing public-private technical working group with industry, academia, and standards bodies to pilot and evaluate advanced compliance technologies.	Continuous engagement with the private sector ensures that FinCEN's rules keep pace with innovation and that compliance tools remain effective, privacy-preserving, and economically efficient. This collaboration would strengthen AML/CFT investigations, reduce false positives, and alleviate the compliance burden on financial institutions while upholding privacy and data-protection standards.

Exhibit B- Full Response to Questions for Comment

1. In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem? What key trends in illicit finance risks have financial institutions observed in the digital asset ecosystem?

- **The question posed is on digital asset systems specifically, but the OIDF is concerned with the broader lens of illicit finance where:**
  - MSFT estimates there is $10T in global cybercrime annually, and the NSA forecasts this will grow to $20Tglobal cybercrime by 2035.
  - In the US, the GAO also detected that there is $233-512B in Federal benefits fraud annually from 2018-2022, https://www.gao.gov/products/gao-24-105833
  - The recent Aspen Institute National Strategy to Prevent Fraud and Scams highlights the harm that fraud brings to everyday Americans and businesses. This report highlights the critical role of standards to better protect the American economy from foreign adversaries. https://openid.net/oidf-supports-national-strategy-on-fraud-and-scam-prevention/
- **The single greatest risk facing the newly regulated stablecoin ecosystem under the GENIUS Act is not novel blockchain activity, but the pervasive failure to establish high-assurance identity at the point of onboarding and transaction. This failure directly jeopardizes the ability of Permitted Payment Stablecoin Issuers to comply with the new Bank Secrecy Act (BSA) obligations imposed by Section 4(5)(A) of the GENIUS Act.**
  - FINCen analysis of all 2012 suspicious activity reports (SARs) found that $212B in financial crime is directly linked to gaps in identity infrastructure https://www.fincen.gov/news/news-releases/fincen-issues-analysis-identity-related-suspicious-activity#:~:text=Report%20examines%20suspicious%20activity%20tied,as%20opening%20and%20accessing%20accounts. It is this family of risks that we see as critical to resolve, establishing high level assurance that an individual is who they say they are and that an entity is who they say they are —that Permitted Payment Stablecoin Issuers will struggle to overcome using outdated, manual processes. The risk is not unique to digital assets, but the opportunity to address it at scale, through the implementation of standardized digital identity and security frameworks, is unique to this moment of new regulation.Without trust in who a counterparty is in any given transaction, digital asset or otherwise, criminals will exploit every gap made available to them.
- **As a standards body that specializes in standards at the intersection of identity and financial services (and identity and other use cases), our concern is on the superset of fraud more than solely digital asset illicit activity**.
  - There are technologies that are uniquely well placed to scan blockchains and crypto networks for anomalies and to trace known crimes, and we will not comment on them as that is not our domain expertise.

- **Our expertise is on the specifications that can help shore up this core identity infrastructure to enable Permitted Payment Stablecoin Issuers to achieve compliant scale.** We will focus our comments on the specifications that can help shore up this core infrastructure inclusive of but broader than digital assets:
    - **OpenID for Verifiable Credential Issuance, OpenID For Verifiable Presentation, the High Assurance Interoperability Profile**: Standards for verifiable credentials which have been adopted by 37 countries, and they are in active use by 1.3M Americans already.
    - **OpenID Connect and FAPI 2.0:** Standards for the secure exchange of information between and within entities
    - **OpenID Federation**: Universal trust discovery and management protocol for different ecosystems (federated and verifiable credential-based).
    - **OpenID for Identity Assurance**, used to exchange assurance information between parties such as NIST SP 800-63-4 Digital Identity Guidelines and the risk based levels of assurance defined by them.
    - **Shared Signals Framework, CAEP, RISC:** Standards for the sharing of signals amongst ecosystem participants, within and across organizations, public and private
- **One of the least discussed but most pervasive risks and vulnerabilities is also one of the US's greatest strengths, our ability to innovate to develop new products, services, and standards.** But innovation itself can be the enemy of robust security infrastructure and collaboration amongst industry experts. This is a key theme in JPMC CISO Patrick Opet's Letter to Third Party SaaS providers:
    - Software providers must prioritize security over rushing features. Comprehensive security should be built in or enabled by default.
    - We must modernize security architecture to optimize SaaS integration and minimize risk.
    - Security practitioners must work collaboratively to prevent the abuse of interconnected systems.
    - Source https://www.jpmorganchase.com/about/technology/blog/open-letter-to-our-suppliers.
    - OIDF sees several opportunities to leverage innovation while shoring up baseline identity and security infrastructure, and that includes, an "opinionated" view on reference architecture that layers the most mature and proven standards (from OIDF and peer standards bodies) and offers best practices on the configuration on those standards.
        - No government entity and no financial institution should be deprived of advice on best practices, critical information should be made broadly available so no financial institution is "left behind," and that entity and their customers become the "weakest links."
        - In this spirit, OIDF encourages government to enable marketplaces where companies are competing on user experience and features and not on baseline security best practices that can be delivered by standards. Supporting a common high bar for security has ecosystem wide benefits.

- **Another critical vulnerability is the lack of digital public infrastructure.** US digital asset providers cannot rely on digital public infrastructure as they can today and will be able to do more swiftly in other countries.
    - In a US society that is profoundly digital, it is unusual that tens of other countries outstrip the US in digital identity infrastructure.
        - India's Aadhaar with its 1.4B users, Brazil with its Gov.Br digital identity program, are some of the largest scale but there are also Nigerian NIMC programs, Kenyan digital identity programs, Estonia digital identity, BankID in Norway, BankID in Sweden, and Singpass in Singapore to naem a few.
        - In total 60 countries are pursuing digital identity programs
        - 38 jurisdictions (from global north and global south) have chosen OIDF's OpenID for Verifiable Credentials to underpin their digital identity wallet and verifiable credential, national identity program. This we know because we partner directly with regions and individual jurisdictions, their government decisions makers and architects to support and help scale their programs. Unilaterally these jurisdictions seek to ensue they benefit from the security, interoperability, scale and privacy preserving aspects of OIDF specifications, and the specifications of our liaison partners that combine to form robust digital infrastructure.
            - OIDF has no single counterparty in the US administration with whom we can collaborate on similar terms to how we support other countries. We welcome the opportunity to provide similar support to the US government, and help inform your due diligence and any future national rollout.
    - **In the US, progress on digital identity infrastructure is slowed by the dependence on state level issuance of credentials led by state and private company investment, with modest federal support.**
        - There are now 18 US states issuing mobile driving licenses, and acceptance by TSA/ DHS at hundreds of the most travelled airports in the USA.
        - The American Association of Motor Vehicle Administrators indicates that over 40% of Americans could access a digital identity credential if they would like to do so. This coverage will increase, as state enabling laws are passed and states complete and launch programs that are already funded but not yet live or out of pilot phases. US states will continue to launch a range of wallets that are state controlled (eg in Utah, Colorado, Utah), as well as issue state credentials into wallets controlled by third parties like Apple Wallet, Google Wallet and Samsung Wallet enabled identity credentials.
        - However there are material barriers to rapid US adoption of this technology.

        - There is limited financial capacity within each state to fund a program and to level up the skills and security expertise needed to issue and maintain a digital identity program.
        - There is no material financial or expertise support from the Federal government, yet.
        - Bills with broad bilateral support went through Congress and were at the cusp of passing. Since they never passed, the federal focus on a national strategy and state/jurisdiction level funding has fallen short. As a result, US adoption and this critical security foundation is moving at a slow pace, radically slower than the pace of other jurisdictions with a clear national strategy and funding.
        - Support has been constrained to vital but overall modest investments by NIST NCCoE mDL and NIST SP800-63-4 projects and the funding and rollout of TSA/DHS acceptance of mDLs, for the “champion use case” of using an mDL to pass a TSA security checkpoint.
    - **One of the primary barriers to the pervasive use of digital identity infrastructure is the barriers to adoption in FI regulated use cases - for both traditional finance and for digital asset use cases.**
        - OIDF has partnered with NIST NCCoE Project to help break down the barriers to US FI adoption of Mobile driving licenses/ verifiable credentials
        - These reports referenced below address how mDLs do meet regulatory requirements, and how to further increase FI confidence in acceptance
            - OIDC_KYC Metadata requirements
            - OIDF Extended eKYC considerations
    - **The lack of digital public infrastructure poses a significant, unnecessary compliance cost burden on Permitted Payment Stablecoin Issuers as they attempt to meet new BSA requirements under the GENIUS Act.** In other countries, digital public infrastructure supports high-assurance identity verification at negligible cost. In the US, the reliance on state-level issuance and the lack of federal backing forces the newly regulated stablecoin issuers to shoulder the full cost of identity assurance, hindering competitive entry and scalability. The **GENIUS Act** provides an opportunity for Treasury to signal acceptance of standards-based digital identity credentials. **This is one of the primary barriers to the pervasive use of digital identity infrastructure for regulated digital asset use cases, which must be overcome to ensure compliant, widespread stablecoin adoption.** Just as an mDL can be used to “open a bank account” so too can an mDL be used to open a crypto currency account or authorize a digital asset transaction *by a Permitted Payment Stablecoin Issuer* with high assurance and compliance with law.
- **The NIST NCCoE project for “Opening a Bank account” shows how a bank or other financial institution can consume a mobile driving license, and integrate it into its user experience and verification procedures.**

- The UX and user experience of using an mDL to “open a bank account” is fantastic, removing material friction for the user and simplifying the process for FIs. The technology meets CIP requirements, and transactions can be processed at scale using the NIST hosted verifier (open source code that can accept many mDLs concurrently and validate the public keys and process the data on the mDL for bank transaction decision making).
- However, many financial institutions are still nervous to invest in and accept digital identity credentials because they do not understand how they comply with US CIP/KYC laws by default.
- A description of the NIST NCCoE project and the feedback is presented in this report: https://pages.nist.gov/nccoe-mdl-project-static-website/building_mdl_assurance/building_mdl_assurance.html
- For this body of work, the OIDF has not only been a NIST NCCoE CRADA participant, but also partnered with NIST to co-host 9 interop sessions on the OpenID for Verifiable Presentation and OpenID for Verifiable Credential Issuance specifications culminating in these announcements validating the interoperability of the specs in May and July 2025, and both specs have now achieved Final status meaning they are mature, proven and stable.
    - May Interop A Global First: OpenID Foundation Demonstrates Real-World Interoperability of New Digital Identity Standards
    - July Interop OpenID Foundation demonstrates real-world interoperability of new Digital Identity Issuance Standards
- Just as an mDL can be used to “open a bank account” so too can an mDL be used to open a crypto currency account or authorize a digital asset transaction with high assurance and compliance with law. The most savvy members of the digital asset community know that digital identity credentials can help them scale their businesses and avert financial crime, but they are reliant on the identity community to collaborate with the government to unblock momentum in the digital identity domain space - then they can benefit.

2. What innovative or novel methods, techniques, or strategies related to APIs 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 APIs?

The lack of digital public infrastructure poses a significant, unnecessary compliance cost burden on Permitted Payment Stablecoin Issuers as they attempt to meet new BSA requirements under the GENIUS Act. In other countries, digital public infrastructure supports high-assurance identity verification at negligible cost. In the US, the reliance on state-level issuance and the lack of federal backing forces the newly regulated stablecoin issuers to shoulder the full cost of identity assurance, hindering competitive entry and scalability. The **GENIUS Act** provides an opportunity for Treasury to signal acceptance of standards-based digital identity credentials. **This is one of the primary barriers to the pervasive use of digital identity infrastructure for regulated digital asset use cases, which must be overcome to**

ensure compliant, widespread stablecoin adoption. Just as an mDL can be used to "open a bank account" so too can an mDL be used to open a crypto currency account or authorize a digital asset transaction *by a Permitted Payment Stablecoin Issuer* with high assurance and compliance with law.

- The OIDF starting point is to consider digital assets and the illicit activity risks associated with them to be broadly similar to the illicit activity and risks posed by other types of financial assets.
- Although the traditional and digital assets themselves and the way those assets are exchanged are different, they face the same challenges as traditional financial services to establish:
    - a person is who they say they are
    - an entity is who they say they are
    - comply with regulations such as CIP/KYC obligations.

In these comments we will highlight three families of standards that could support robust US financial and identity infrastructure:

1) **OpenID for Verifiable Credential Issuance, OpenID For Verifiable Presentation, the High Assurance Interoperability Profile**: Standards for verifiable credentials which have been adopted by 37 countries, and they are in active use by 1.3M Americans already.
2) **FAPI 2.0:** Standards for the secure exchange of information between and within entities
3) **OpenID Federation**: Universal trust discovery and management protocol for different ecosystems (federated and verifiable credential-based).
4) **OpenID for Identity Assurance**, used to exchange assurance information between parties such as NIST SP 800-63-4 Digital Identity Guidelines and the risk based levels of assurance defined by them.
5) **Shared Signals Framework, CAEP, RISC:** Standards for the sharing of signals amongst ecosystem participants, within and across organizations, public and private

To elaborate on the first
(1) For OpenID For verifiable credentials, we refer to three documents.

A. **Utah State request for information on their SEDI initiative**, our recent submission which comments on state level approach, and includes many of the latest facts around the benefits of the specifications, their US and global adoption. (attached)
B. Two papers that elaborate on the use of OpenID for Verifiable Credentials and precisely how they can be used to meet current CIP regularly requirements, KYC requirements and how some gaps can be closed to further scale their use by FIs in particular. This would include the use for digital assets use cass. See attached the following detailed proposals in development by the eKYC & IDA WG at the OIDF:
    - **OIDC_KYC Metadata requirements**
    - **OIDF Extended eKYC considerations**

To elaborate on the second:

(2) Deterring risks in the movement of information between entities in an ecosystem
In this context, OIDF hears from many of the government and private sector ecosystems looking for not only open standards that meet their requirements, but opinionated, reference architecture (e.g. version 0.1) that will help their entire ecosystems resist attack at scale.

It is in this context that many ecosystems have selected FAPI 2.0 for open banking and open data deployments, including the Financial Data Exchange in the US
We believe US FIs will start deploying FAPI 2.0 internally and externally to rationalize their SaaS architecture, and avert the porous surface introduced by a wide array of services with disparate security profiles. FAPI 2.0 offers a standardized security profile, to ensure a single high bar for all entities or services that need to interoperate. Below is a chart of leading ecosystems in the US and abroad that have adopted FAPI:

Ecosystems Selecting FAPI for secure data sharing	Public Sector or Private Sector Led	Selected FAPI	Require FAPI	Deployed FAPI
US Financial Data Exchange - Open Finance - FAPI 2.0 is the approved "blue" profile	Private sector led	◉	◉	◉
United Kingdom - Open Banking	Government sector led	◉	◉	◉
Australia - Treasury, Data Standards Body, Open Data	Government sector led	◉	◉	◉
Australia - ConnectID (identity data, bank-led consortia)	Private sector led	◉	◉	◉
Brazil Open Finance	Government sector led	◉	◉	◉
Saudi Arabian Monetary Authority - Open banking	Government sector led	◉	◉	◉
United Arab Emirates - Open Banking	Government sector led	◉	◉	◉
Chilean Ministry of Finance - Open banking	Government sector led	◉	Expected 2026	Expected 2026
Colombia - Open banking	Government sector led	◉	Expected Nov 2025	Expected Nov 2025
Norwegian HelseID - Health data,	Government sector led	◉	◉	◉

Ecosystems Selecting FAPI for secure data sharing	Public Sector or Private Sector Led	Selected FAPI	Require FAPI	Deployed FAPI
US Financial Data Exchange - Open Finance - FAPI 2.0 is the approved "blue" profile	Private sector led	◉	◉	◉
United Kingdom - Open Banking	Government sector led	◉	◉	◉
Australia - Treasury, Data Standards Body, Open Data	Government sector led	◉	◉	◉
Australia - ConnectID (identity data, bank-led consortia)	Private sector led	◉	◉	◉
Brazil Open Finance	Government sector led	◉	◉	◉
Saudi Arabian Monetary Authority - Open banking	Government sector led	◉	◉	◉
OIDF/ HelseID blog post				
German Verimi - (private, open banking consortia)	Private sector led	◉	◉	◉
Canada - Open Banking	Government sector led	Expected	Expected	Expected

Notes:
(1) Other G20 and global south countries have selected FAPI 2.0, but it is confidential to OIDF, not yet public information.
(2) OIDF is an observer to the Bank of International Settlements "Aperta Project," given the fit of FAPI 2.0 to support supply chain and transaction banking use cases.

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

- See the reports attached for how mobile driving licenses meet US financial regulatory requirements to enable financial transactions securely. Although these reports are related to traditional finance to open a bank account, the work can equally apply to digital asset use cases:
  - OIDC_KYC Metadata requirements
  - OIDF Extended eKYC considerations

(b) How are financial institutions using API 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 API tools with other existing or previous tools used for similar purposes.

- Financial institutions typically with pilot and then phase in technologies with proven benefits
- That methodology can be used to introduce and pilot acceptance of OpenID for Verifiable Credential or Mobile driving licenses for a narrow population, learn and then scale it across the entire consumer estate and a wider array of use cases.
- Integrating mDL/VDC acceptance, enabled by OIDF standards, is the most cost-effective path to high-assurance CIP compliance for Permitted Payment Stablecoin Issuers. For new market entrants under the GENIUS Act, achieving compliance cost-effectively is essential for viability. The ability to use VDCs as the first step in a CIP/KYC "waterfall" provides the lowest-cost, highest-assurance verification method, freeing up resources to focus on higher-risk customers. Treasury should explicitly recognize the economic benefit this provides to newly-regulated issuers.
- For example, if the financial institution had assurance the mDL met CIP and KYC, then it would be the first step in any CIP/KYC “waterfall.”
    - “Does this user have an mDL/mID?
        - If yes, check it, verify it, and complete the transaction.
        - If not, complete all other steps in the waterfall.”
    - Using this approach, FIs can focus their resources on verification of users without high assurance credentials.
- See the reports attached on the benefits and playbook to accelerate mDL/mID acceptance across US FIs
    - OIDC_KYC Metadata requirements
    - OIDF Extended eKYC considerations
- When standards are deployed, conformance can be achieved at scale
    - It is vital when using standards that the work carries through to testing for conformance to those standards, otherwise the systems remain:
        - Vulnerable to human error during launch
        - Risks as implementers update systems which create unexpected breaking changes that will undermine security and interoperability if not detected in real time.
    - OIDF specifications are free to use, and free to contribute to, and OIDF offers free open source tests to help ensure implementers are benefiting from the specs The only cost is if an entity or ecosystem wants to deploy conformance, 4k implementers have used OIDF conformance services to date: https://openid.net/certification/ and an accreditation service will be launched in Q2 2026 to support scale deployments

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

Obstacle (Issue Identified)	Recommendation (Proposed Solution)	GENIUS Act Linkage (The Improvement)
1.Regulatory/ Supervisory Ambiguity in CIP/KYC	**Recommendation 1.1 (API-Enabling Guidance):** Treasury/FinCEN should issue guidance that explicitly recognizes **Verifiable Digital Credentials (VDCs)** that meet standards (e.g., NIST SP 800-63-4 IAL2, OIDF profiles) as constituting "**documentary evidence**" for CIP purposes.	This is the single largest barrier to the scaled, low-cost compliance needed for the new class of **Permitted Payment Stablecoin Issuers** under **Section 4(5)(A)(v) of the GENIUS Act**. Clarifying VDCs as documentary evidence will unlock the use of API-based identity proofing and enable stablecoin issuers to meet their new BSA/AML mandates efficiently.
2. Operational Siloing in Risk Mitigation	**Recommendation 2.1 (Standardized Risk APIs):** Mandate or strongly incentivize the use of API standards, such as the **OpenID Shared Signals Framework (SSF)**, for the real-time, standardized exchange of risk signals (e.g., account takeover, PII compromise) between regulated entities.	The **GENIUS Act** introduces a new, interconnected stablecoin ecosystem. Relying solely on internal, legacy systems is an operational obstacle. APIs using the SSF standard are the fastest, most effective way for **Permitted Payment Stablecoin Issuers** and other FIs to share the real-time intelligence necessary to mitigate fraud related to stablecoin accounts.

3. Legislative Inertia in the Travel Rule	**Recommendation 3.1 (Travel Rule Modernization):** The Travel Rule (31 CFR § 1010.410(f)) must be updated to explicitly permit compliance via API-based, privacy-enhancing methods, allowing the transfer of cryptographically verifiable proof of required originator/beneficiary information instead of unencrypted PII.	The current Travel Rule creates a legislative obstacle for API-driven, privacy-preserving digital asset transfers. Modernizing this rule will allow **Permitted Payment Stablecoin Issuers** to achieve full compliance with data-sharing requirements under **Section 4(5)(A)** while simultaneously upholding the principle of data minimization, which is vital for building public trust in regulated digital assets.
4. Lack of a Common API Security Baseline	**Recommendation 4.1 (Mandate High-Assurance API Standards):** Federal supervisors should require the use of high-assurance security profiles—such as **FAPI 2.0**—for all APIs used by **Permitted Payment Stablecoin Issuers** and their third-party identity partners to secure the movement of customer data.	The complexity of digital asset services increases the attack surface. **FAPI 2.0** provides a common, high-security baseline for financial APIs. Mandating its use will remove the operational obstacle of disparate security controls, ensuring that the new regulatory landscape introduced by the **GENIUS Act** is built upon a resilient and standardized security foundation, consistent with OIDF's reference architectures.
5. Absence of Legal Recognition for Partially Anonymous Authentication Current AML regulations lack clear provisions for controlled anonymity and unlinkability required for privacy-preserving compliance.	**Recommendation 5.1:** Treasury should amend 31 CFR § 1020.220 to explicitly permit authentication models compliant with ISO/IEC 29191 where a designated opener can re-identify claimants under lawful process. This balances law-enforcement visibility with the **GENIUS Act's** goal of privacy-preserving innovation.	

- The technologies are available to secure US FI architecture. The following APIs are proven and mature at US and global scale, and can be used to undermine US financial infrastructure:
    - **FAPI 2.0 for exchange of data** in a wider range of use cases. FAPI 2.0 is the railway track on which any cargo can be exchanged within a single financial entity, across a financial ecosystem (e.g. open banking, open data) or across other open data deployments (e.g. Open health, open insurance)
    - **OpenID For Verifiable Credentials** for users to be able to present high assurance credentials
    - **Shared Signals for Risk Information Sharing** to be able to circulate across organizations information on sessions/accounts that are high risk. This recent report by the OIDF explains how Shared Signals can be combined with STIX and TAXI to empower FIs to make stronger choices: https://openid.net/how-ssf-caep-and-stix-taxii-secure-different-front/ Shared signals was recommended by CISA as a material recommendation in the wake of the recent Microsoft Breach, as advice for cloud service providers to mitigate risks at scale within and between entities.
- Many regulatory and legislative leaders are not familiar with the available identity and security standards, what benefits they deliver, and how to incentivise their use across the economy.
    - To help close this knowledge gap, OIDF has held numerous briefing sessions over the past 3 years to brief all the financial regulators including the head of the NY Fed, FinCEN, Treasury, OCC, and partnered at length with NIST to mature SP 800-63-4 Digital Identity Guidelines and NIST NCCoE on mDLS
    - However the US still lacks a national strategy for the scaling of digital identity credentials to realize their benefits as a public good, and ensure they can enable new technologies like digital assets and Agentic AI safeguards
    - Beyond the federal level, there are thousands of US federal and state level legislators, and thousands of regulators
        - There are 67 US State/ jurisdictions that would need to issue State/jurisdiction level credentials… of whom only 18 have launched so far.

- Many financial leaders are not familiar with the available identity and security standards, what benefits they deliver, and how they fundamentally benefit their P&L and the FI ecosystem wide benefits
    - The number of US financial institutions is ~10k, with then thousands of executives, product specialists, regulators, and developers all of whom need to develop familiarity with a new technology and what it means to their role and their organization and their P&L
- The number of technologists fluent in leading global identity standards are dwarfed by the number of decision makers in the US FI and government regulatory bodies

- There are only hundreds of digital identity experts globally, and they spend the majority of their time developing technical standards, not explaining how and why governments or FIs should adopt them as critical infrastructure.
- Identity experts like those in the OIDF do not have the capacity to brief all US regulatory, legislative and financial decision makers to help them understand the fundamental role the digital identity APIs like verifiable credentials, security profiles and shared signals deliver
- Identity experts and the organizations that employ them, will also go towards projects and jurisdictions where there is clear demand. For example, there are 60 countries pursuing digital identity, and one of the fastest moving is the EU. This draws resource momentum and capacity towards non-US markets. We are also seeing in action how the decisive approach to architecture from the EU is leading others to follow their lead: Western Balkans, UK, Switzerland to name a few.

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

Step the U.S. Government Should Take	Rationale and Linkage to the GENIUS Act (The Improvement)
1. Explicitly Sanction Verifiable Digital Credentials (VDCs) as "Documentary Evidence" for CIP Compliance. Action: Treasury/FinCEN must issue immediate, unambiguous guidance clarifying that VDCs—issued by trusted authorities and utilizing approved technical standards (e.g., OIDF's OpenID for VC and NIST SP 800-63-4 IAL2)—constitute **"documentary evidence"** for CIP requirements.	**GENIUS Act Link:** This step directly addresses the primary regulatory obstacle for **Permitted Payment Stablecoin Issuers** under **Section 4(5)(A)(v)**, which subjects them to new BSA/AML obligations. Without this clarity, these new entities cannot effectively leverage API-driven identity solutions, forcing them to rely on outdated, high-cost, and less secure manual processes. This is the foundation for effective, risk-based API adoption.
2. Mandate the Use of High-Assurance API Security Standards. Action: Federal regulators (Primary Federal Payment Stablecoin Regulators) should require that all APIs used by **Permitted Payment Stablecoin Issuers** for transmitting sensitive customer data, account information, or financial transaction commands conform to a recognized high-security standard, such as **FAPI 2.0** (Financial-grade API Security Profile).	**GENIUS Act Link:** The security of the payment stablecoin ecosystem is paramount. Requiring **FAPI 2.0** establishes a single, non-negotiable security baseline for the data flow *between* regulated entities. This facilitates **risk-based adoption** by ensuring API integrations are uniformly secure, reducing the collective systemic risk and protecting customers who hold

	payment stablecoins issued under the Act.
3. Establish a National Standard for Real-Time Risk Signal Exchange. Action: The U.S. government should formally recognize and promote an open standard, such as the **OpenID Shared Signals Framework (SSF),** as the preferred or mandatory API specification for real-time risk intelligence sharing (e.g., account takeover and anti-fraud alerts) among **Permitted Payment Stablecoin Issuers** and other financial institutions.	**GENIUS Act Link:** APIs are essential for detecting illicit finance *in real-time*. This step enables the new stablecoin regulatory class to move beyond reactive SAR filing to **proactive mitigation**. The standardization of risk communication through OIDF's SSF will allow **Permitted Payment Stablecoin Issuers** to interoperate seamlessly with the broader financial sector, bolstering the integrity of the U.S. financial system that the **GENIUS Act** seeks to strengthen.
4. Fund Interoperability and Pilot Programs for Compliant APIs. Action: Congress and Treasury should fund programs, potentially leveraging the NIST NCCoE, specifically tasked with creating and sharing open-source reference architecture and API implementations that demonstrate how **Permitted Payment Stablecoin Issuers** can meet their CIP/KYC and Travel Rule obligations using open identity and security standards.	**GENIUS Act Link:** Adoption of innovative APIs is hindered by the high initial cost of proof-of-concept and legal review. Government-funded reference implementations and pilot projects—focused on the new compliance requirements of the **GENIUS Act**—would drastically reduce the operational barrier to entry, accelerating the safe and risk-based adoption of compliant API technologies across the entire stablecoin market.

Recognize Partially Anonymous, Partially Unlinkable Authentication as Permitted under GENIUS Act Section 4(5)(A)	Action: FinCEN should issue interpretive guidance clarifying that digital-identity frameworks based on OpenID Connect and OpenID Federation with ephemeral subject identifiers qualify as acceptable privacy-enhancing authentication mechanisms under CIP/KYC obligations, so long as they retain a designated re-identification path for law-enforcement access. This guidance would implement ISO/IEC 29191 requirements and support risk-based adoption of API-enabled privacy controls envisioned by the GENIUS Act.

- As noted in our cover letter, our recommendations are focused on building more resilient architecture and not just detecting downstream illicit activity.
- To accomplish these wider goals we regularly work on multistakeholder projects in the US and more broadly. .
    - Efforts like the NIST NCCoE on Mobile Driving Licenses to "open a bank account" using Verifiable credentials, is a good example. The project convenes industry participants and pilot the usage of the technologies to mobilize early adopters, establish tools and offer assurance of compliance. Since NIST is already piloting the OpenID for Verifiable Credentials APIs, then the next step would be other incentives to motivate usage.
    - For APIs like the Shared Signals Framework, and the CAEP and RISC schema (for account and session based risk signals) these could also benefit from a NIST NCCoE or equivalent project to scale up its use by the US Government and private sector experts and stakeholders. Many private companies like Apple, Google, CISCO, SGNL, Sailpoint and Okta are already supporting Shared Signals and deploying them, however the technology is still earlier on the adoption curve.
    - The OIDF is also an official observer of the Bank of International Settlements "Project Aperta" to address cross border open data for transaction banking and supply chain use cases, with a second phase inclusive of consumer facing use acses to come soon.

(e) Treasury will evaluate APIs and consider their impact based on the research factors identified in the GENIUS Act.19 Provide any information pertinent to those factors.

Research Factor (Expected Statutory Focus)	Information Pertinent to the Factor (Impact of OIDF API Standards)
1. Security and Fraud Mitigation	**OpenID FAPI 2.0 & Shared Signals Framework (SSF) APIs** deliver a unified, high-assurance security standard. FAPI 2.0 is selected globally for open banking and open data to rationalize porous SaaS architecture. Impact: These APIs reduce cybercrime exposure by standardizing security profiles across the stablecoin ecosystem and enabling Permitted Payment Stablecoin Issuers to exchange real-time risk intelligence (SSF), which is crucial for mitigating account takeover and synthetic identity fraud before it affects assets regulated by the GENIUS Act.
2. Interoperability and Scalability	**OpenID for Verifiable Credential (VC) Issuance & Presentation APIs** are the connective tissue for a "network of networks." They are utilized by 37 countries for digital wallet deployments. **Impact**: This global scale and proven interoperability is essential for the future of digital assets. By adopting OIDF standards, the U.S. ensures that **Permitted Payment Stablecoin Issuers** are not limited to a closed, domestic-only system, but can achieve global scale and align with international standards like FATF Digital ID Guidance and EU eIDAS 2.0, supporting the global leadership objective of the GENIUS Act.
3. Efficiency and Cost Reduction	**Verifiable Credential (VC) API-based Verification** is the lowest-cost, highest-assurance method for Customer Identification Program (CIP) compliance. **Impact:** For the new Permitted Payment Stablecoin Issuers facing new BSA/AML mandates, VCs eliminate the high per-check cost of traditional data bureaus and manual document review. Treasury's sanctioning of VC APIs facilitates effective, risk-based adoption by making high-integrity identity verification economically viable for all market participants, fostering the national innovation championed by the GENIUS Act.
4. Privacy and Data Minimization	**Verifiable Credential and Privacy-Enhancing Technology (PET) APIs** enable attribute-based verification (e.g., proving "over 21" or "US Person" without sharing the full date of birth or address). **Impact:** These APIs directly implement the principle of data minimization, allowing **Permitted Payment Stablecoin Issuers** to comply with CIP/AML laws without over-collecting and warehousing unnecessary Personally Identifiable Information (PII). This reduces the issuer's data breach liability and fosters consumer trust in the regulated stablecoin products established by the **GENIUS Act.**

3. What innovative or novel methods, techniques, or strategies related to AI 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 AI? Please describe the use of AI to conduct analysis of transactional data, including

transactions that occur on blockchains, and to identify complex illicit financial networks, as well as key lessons learned from use of AI in this context.

The OpenID Foundation just completed a report on the intersection of AI and Identity, which has been picked up by 20 media outlets in less than a week. This paper characterizes the opportunities and risks associated with AI + Identity. The key message here is that AI opens up a wide range of risks, and those risks will be exploited at scale until robust digital identity infrastructure is deployed, which will include verifiable credentials held by individuals to assert their identity definitively and avert risks of deep fakes/social engineering, and for beneficial owners of companies to assert their identity as part of entity-linked transactions, and for assurances that the entity is who it says it is as well: https://openid.net/new-whitepaper-tackles-ai-agent-identity-challenges/

In this context, digital assets are just another type of relying party use case. Agentic AI will both enable and lead to illicit activity across all sectors and verticals of which digital assets it is just one type. The core requirements to mitigate the risks are the broadly the same, and not unique to the digital asset domain space. That said, if digital identity infrastructure is enabled at scale, it can accelerate the growth of digital assets and blockchain technologies.

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

- No further comment see above.

(b) How are financial institutions using AI 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 AI tools with other previous or existing tools used for similar purposes.

- No further comment see above.

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

- No further comment see above.

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

- No further comment see above.

(e) Treasury will evaluate AI and consider its impact based on the research factors identified in the GENIUS Act.20 Provide any information pertinent to those factors.

- No further comment see above.

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.

- See comments above on the three most relevant API Families already used at scale that merit use across industry categories inclusive of but not limited to digital asset use cases. These are all mature specifications that can be deployed at scale now, but they are still novel in that they are still moving up the adoption curve with higher penetration in some use cases more than others…but all can be relevant to help scale digital asset adoption:
    - OpenID Connect and FAPI 2.0
    - OpenID for Verifiable Credentials
    - OpenID Federation
    - OpenID For Identity Assurance
    - Shared Signals

(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.

- The primary consideration for any financial institution in setting up an AML/CFT "waterfall" is to take all their users through the lowest cost highest assurance checks first, and take as few users as possible through the most expensive checks (E.g. in branch ID verification)
- As mentioned earlier, we suspect that FI executives, product leaders, legal and compliance officials will all support the use of digital identity credentials as the very first check in any waterfall. It is a rational decision to benefit from the lowest possible costs and highest possible assurance check. However, they will not start integrating acceptance until they understand how the technology complies with their CIP/KYC obligations.
- Recently US regulators issued advice that "prefilled" data would comply with regulatory requirements; it was interesting to note that Mobile driving licenses – issued by 18 states – have not benefited from a similar clarification statement. Such clarity would help motivate FI investment and acceptance
    - Although it is not common practice for regulators to explicitly state that specific technologies are compliant, in this case, unblocking FI adoption and scaling the

  - use of verifiable credentials would likely play a material role in adoption beyond the organic pace we are observing now.
  - It would likely also help ensure a more robust infrastructure emerges where verifiable credentials become common place and a material enabler of trust in FI/ digital asset transactions, and other transaction types

(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.

- No comment

(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.

- Shared Signals, CAEP and RISC are specs that can already be used to exchange information on risky accounts and sessions in real time, which could protect both financial transactions generally and digital asset transactions.
- The potential for use of Shared signals in the FI domain space is explored in this blog post, where Shared Signals is aligned to commonly deployed STIX and TAXII standards. The main difference is that Shared signals offers real time risk signals on account and session information that STIX and TAXII do not cover. As the blog post illuminates, these standards are complementary, and the OASIS standards body and OIDF stand ready to progress this work in partnership with the USG and US FIs. https://openid.net/how-ssf-caep-and-stix-taxii-secure-different-front/

(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?

- No further comment

(e) Treasury will evaluate digital identity verification and consider its impact based on the research factors identified in the GENIUS Act.21 Provide any information pertinent to those factors.

- No further comment

5. What innovative or novel methods, techniques, or strategies related to blockchain technology and monitoring 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 blockchain technology and monitoring? Please describe how financial institutions are integrating information from blockchain analytics with off-chain data and mention any key challenges associated with using

blockchain analytics (e.g., obfuscation tools and methods that can complicate tracing and assessing confidence in attribution or complexities inherent in cluster analysis).

- No comment.

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

- No comment.

6. What innovative or novel methods, techniques, or strategies related to any other innovative technologies such as cryptographic protocols and other privacy-enhancing tools, cloud-based solutions, on-chain compliance tools, oracles, 23 or new verification tools for smart contracts 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 these other innovative technologies?

- OpenID for Verifiable Credentials together with mobile driving licenses (mdocs) allows for the privacy enhancing release of PII to Financial institutions. The OpenID4VCI and OpenID for VCI and the credentials themselves leverage cryptography to issue credentials, present credentials in person and online, and ensure only the relevant information is presented to the relying party.
- Treasury and FinCEN should encourage the development of reference implementations demonstrating OpenID flows that achieve ISO/IEC 29191 compliance. These pilots could be conducted under NIST NCCoE to validate that partially anonymous, partially unlinkable authentication meets AML/CFT supervisory requirements while preserving citizen privacy and interoperability with international standards (e.g., EU eIDAS 2.0 Wallets and FATF Digital ID Guidance).

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

- No further comment

(b) How are financial institutions using other innovative technologies 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 other innovative technologies with other existing or previous tools used for similar purposes.

- No further comment

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

- No further comment

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

- No further comment

(e) Treasury will evaluate other innovative technologies and consider their impact based on the research factors identified in the GENIUS Act.24 Provide any information pertinent to those factors.

- No further comment