Comment of Coin Center to FinCEN and OFAC on PPSI AML/CFT and Sanctions Program Requirements

June 9, 2026
FINCEN–2026–0100
OFAC_FRDOC_0001

To whom it may concern:

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin and Ethereum. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain networks. We do this by producing and publishing policy research from academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

We thank the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) for the opportunity to comment on *Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements* pursuant to the *Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act*.

This rulemaking sits at a dangerous crossroads. Payment stablecoins can become a freer, faster, more open form of digital money, or they can become the backbone of an identity-linked financial surveillance system more comprehensive than anything possible in traditional banking. The difference will turn on how FinCEN and OFAC implement GENIUS.

Coin Center supports effective AML/CFT and sanctions compliance for regulated financial intermediaries. PPSIs should screen their own customers, maintain lawful compliance programs, and respond to lawful orders. But regulators must not use stablecoin issuance as the hook for a broader surveillance mandate over peer-to-peer activity, nor should they push issuers to build databases that link static identity records to permanent public blockchain histories.

The risks are not limited to privacy in the abstract. Overcollection of personal information creates fraud material for criminals, honeypots for hackers, intelligence targets for foreign adversaries, and dossiers for future political abuse. Broad secondary-market monitoring would compound those dangers by turning PPSIs into private surveillance deputies and probabilistic adjudicators of Americans' property rights.

The final rules should draw a clear line. Regulated relationships and lawful orders are appropriate subjects of PPSI compliance. Generalized monitoring, identity-linked blockchain dossiers, and warrantless or process-free freezes of U.S. persons' property are not. FinCEN and OFAC should preserve that line by encouraging privacy-preserving digital identity, data-minimized compliance, targeted technical capabilities, and strong procedural safeguards.

Accordingly, we recommend that FinCEN and OFAC take five high-level courses of action. First, recognize overcollection of sensitive customer information as an operational and AML/CFT risk. Second, expressly permit PPSIs to use privacy-preserving digital identity tools where they produce auditable compliance outputs. Third, create a pilot or safe harbor for data-minimized onboarding. Fourth, consistent with FinCEN's goals, clarify that secondary-market transfers do not create PPSI monitoring, recordkeeping, or Travel Rule obligations merely because they involve a PPSI-issued stablecoin. Fifth, require lawful process and procedural safeguards before making secondary-market freezes affecting U.S. persons.

I. Operational Risks and Innovative Solutions

Coin Center appreciates FinCEN's recognition that PPSIs are best positioned to assess their own ML/TF risks and allocate compliance resources accordingly. We also welcome FinCEN's openness to innovative technologies for combating illicit finance. But FinCEN should make clear that AML/CFT risks are not limited to a PPSI collecting too little information when overcollection can itself create serious risks.

Current customer identification and data-collection practices remain badly outdated. Americans are still expected to send .jpg files of driver's licenses, photos of themselves, and passport scans to open or use financial accounts. These identity signals are trivially forged by sophisticated criminals, meaning the process often achieves little real deterrence. Meanwhile, ordinary customers comply with the ritual, and institutions build comprehensive dossiers about them, their transactions, and their intimate associations. Those dossiers become honeypots for hackers, who can then use the same stolen data to open more accounts, commit more fraud, and launder more money.

The result is a compliance regime that mistakes examiner comfort for public safety. Financial institutions have become so concerned with the risk of disappointing regulators by failing to collect the same invasive but cheap data they have always collected that they may now be creating more illicit-finance risk than they mitigate. A system that forces good actors to overshare, gives bad actors reusable fraud material, and still fails to stop sophisticated criminals is outdated and backwards.

FinCEN should therefore direct PPSIs to consider and, where possible, quantify the operational risks created by collecting and retaining sensitive customer information. Customer identification programs (CIP) should not be judged only by whether they collect enough information to satisfy legacy expectations, but also by whether they create unnecessary fraud, cybersecurity, privacy, and illicit-finance risks through the collection and retention of sensitive personal data.

FinCEN should also explicitly permit and encourage PPSIs to use alternative onboarding methods that preserve privacy and reduce the overcollection of customer data when a PPSI determines that traditional collection and retention practices would increase operational, cybersecurity, or AML/CFT risk. Privacy-preserving digital identity systems, including portable credentials, attribute-based proofs, and dynamic risk-scoring mechanisms, can allow regulated entities to verify relevant facts without exposing full identity details or transaction histories.

Success should not be measured by the volume of information collected. It should be measured by reductions in illicit finance, cybercrime, fraud, and unnecessary risk to innocent users. A modern AML framework should reward institutions that can verify relevant facts with less data, fewer honeypots, and stronger privacy protections.

1. Cybercrime and Fraud

Financial institutions are persistent targets for cybercriminals because they collect and retain the very information criminals need to defeat identity controls.[1] Once personally identifiable

[1] In 2024, the United States experienced 3,158 data compromises impacting 1.35 billion individuals; in 2023, 3,205 compromises impacting 353 million individuals; and in 2022, 1,802 compromises impacting 422 million individuals. Statista Rsch. Dep't, *Number of Data Breaches and Victims in the United States from 2005 to 2025*, Statista (Feb. 15, 2026), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. "In 2024 about 48 percent of all data breach incidents in global organizations involved customer personally identifiable information (PII), thus making it the most frequently breached type of data." Id. Financial services had the most data compromises of any U.S. industry in 2025 with 739 compromises, up from 2024. Identity Theft Res. Ctr., *2025 Data Breach Report* (Jan. 2026), https://www.idtheftcenter.org/wp-content/uploads/2026/01/2025-ITRC-Annual-Data-Breach-Report.pdf.

information (PII) is stolen, it can be used to open accounts, compromise existing accounts, conduct fraudulent transactions, and launder money in the name of an innocent person. As PPSIs become more widely used, they will face the same incentives for attack. The more sensitive customer information they collect and retain, the more valuable a target they become, and the more harm their customers will suffer when that information is compromised.

This is not a speculative risk. The Identity Theft Resource Center's (ITRC) 2025 annual report found that data compromises in the U.S. are transitioning from "mass identity theft… to pervasive identity fraud and scams, where stolen credentials are weaponized with precision."[2] The report also found that criminals increasingly prioritize "static identifiers that facilitate long-term identity fraud over easily replaceable data, such as credit card numbers."[3] Static identifiers include Social Security numbers (SSNs) and driver's licenses, for which there have been drastic increases in compromises over the past five years.[4]

Financial institutions have increasingly been the main targets. A 2024 study out of the University of Brasília, *Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies* reviewed 506 breaches across 274 companies, and found that financial institutions were the most breached and the primary target for malicious actors.[5] This is because a breach at a financial institution does not merely expose ordinary consumer information, but also the information used to pass identity checks, defeat AML/CFT controls, and impersonate legitimate customers.

The National Institute of Standards and Technology (NIST) has recognized the same problem. In its special publication, *Digital Identities—Mobile Driver's License (mDL)*, NIST identified "the need for secure, usable, and privacy-preserving identity solutions" in light of "the emergence of new threats to identity proofing systems."[6] NIST observed that "[f]inancial institutions, who have direct access to money and sensitive personal information, are subject to emerging cyber

---

[2] Identity Theft Res. Ctr., *2025 Annual Data Breach Report* (Jan. 2026), https://www.idtheftcenter.org/wp-content/uploads/2026/01/2025-ITRC-Annual-Data-Breach-Report.pdf.
[3] *Id*. at 9.
[4] ""Social Security Numbers (SSNs): Compromises involving SSNs nearly doubled, from 1,146 in 2021 to 2,236 in 2025." *Id*. at 9. "Driver's Licenses: Jumped from 456 in 2021 to 1,094 in 2025 as the use of driver's license information has increased with the rise of remote transactions." *Id*.
[5] Guilherme A. P. Rodrigues et al., Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies, 16 *Future Internet* 201, 9–10 (2024), https://www.researchgate.net/publication/381199703_Impact_Compliance_and_Countermeasures_in_Relation_to_Data_Breaches_in_Publicly_Traded_US_Companies.
[6] Yee-Yin Choong et al., Nat'l Inst. of Standards & Tech., *Digital Identities: Mobile Driver's License (mDL): Accelerating Development and Adoption of Digital Identity for Financial Institutions*, NIST Special Publication 1800-42A, at __ (Initial Public Draft Mar. 2026), https://www.nccoe.nist.gov/sites/default/files/2026-03/nist-sp-1800-42a-ipd_0.pdf.

threats. Attackers seeking to drain bank accounts, open fraudulent lines of credit, launder money or steal PII, may target financial institution identity proofing systems."[7] Additionally, NIST reported that FinCEN "linked $212 Billion dollars to identity-related suspicious activity in 2021, a figure that reached as much as $394 billion by 2023," and that "inadequate digital identity systems cost institutions an estimated 3.1% of annual revenue."[8]

In several recent reports, FinCEN has identified that weaknesses in identity processes at financial institutions are exploited by impersonating others, exploiting insufficient processes to circumvent verification, and using compromised credentials to gain unauthorized access to accounts.[9] In 2021, about 1.6 million BSA reports—or 42% of roughly 3.8 million total BSA reports—involved identity-related suspicious activity,[10] and that fraud was the most frequently reported illicit finance typology.[11] FinCEN has also identified that "data breaches compromising [PII], synthetic identities, and artificial intelligence (AI) may further enable bad actors to exploit identity processes more easily, quickly, and inexpensively to drive money laundering, fraud, and cybercrime."[12]

And while these hacks and exploitations may harm financial institutions and their AML/CFT efforts, the real victims are everyday Americans who are simply abiding by the process and handing over sensitive information for financial services. Once stolen, personal information can be reused repeatedly over many years for financial gain or other criminal purposes. Federal complaint data show the scale of the problem. In its 2025 *Internet Crime Report*, the FBI reported 67,456 complaints involving personal data breaches and 31,675 complaints involving identity theft through the Internet Crime Complaint Center.[13] The Federal Trade Commission's most recent *Consumer Sentinel Network Data Book* showed that the number of fraud, identity theft, and other reports increased each year—from 860,383 in 2004 and 2,620,931 in 2014 to 6,471,708 in 2024.[14]

These figures show why overcollection should be treated as an AML/CFT risk, in addition to being a privacy concern. Once collected, sensitive personal information becomes a target and a

---

[7] *Id*. at 6.
[8] *Id*.
[9] Fin. Crimes Enf't Network, *Identity-Related Suspicious Activity: 2021 Threats and Trends*, FinCEN Financial Trend Analysis, Jan. 2024, at 1–2, https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf.
[10] *Id*. at 3-4.
[11] *Id*. at 8.
[12] *Id*. at 5.
[13] Fed. Bureau of Investigation, Internet Crime Complaint Ctr., 2025 *Internet Crime Report* 7, https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.
[14]Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* 2024 6 (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.

tool for fraud, cybercrime, account compromise, and money laundering. FinCEN should therefore clarify that a risk-based AML/CFT program does not require PPSIs to collect and retain sensitive personal information beyond what is genuinely necessary, especially where the PPSI reasonably determines that doing so would increase the risk of hacking, identity theft, fraud, or downstream money laundering. FinCEN should also treat good-faith deployment of privacy-preserving digital identity tools as an innovative activity capable of achieving equivalent or better AML/CFT outcomes, provided PPSIs can produce demonstrable compliance outputs.

For PPSIs, the risk is even sharper than it is for many traditional financial institutions. The most valuable stolen identifiers are static: names, dates of birth, Social Security numbers, driver's license numbers, passport information, and biometric templates. In the stablecoin context, those identifiers can become even more dangerous when linked to on-chain transaction data. A breach that connects real-world identity records to blockchain addresses would not merely expose a customer's account-opening file. It could expose a persistent financial graph of payments, counterparties, balances, and associations. The next section explains why that combination makes PPSIs uniquely vulnerable to identity-theft risk and why FinCEN should account for that risk when evaluating PPSI AML/CFT programs.

2. Linking Static Identifiers with On-Chain Data

PPSIs face a distinct identity-theft and privacy risk because stablecoins often move across public blockchains. When static identifiers, such as names, dates of birth, Social Security numbers, driver's license numbers, passport information, or biometric templates, are linked to blockchain addresses, they create a bridge between a person's real-world identity and a persistent public transaction graph.

That linkage can reveal intimate details about a person's life: payments, counterparties, balances, donations, memberships, habits, beliefs, and associations. In the hands of the federal government, that information invites warrantless financial surveillance and political abuse. For example, a hostile administration or agency may leverage this information for discrimination, harassment, debanking, and the chilling of lawful expressive and associational activity. In the hands of a foreign adversary, it can be used to identify dissidents, diaspora communities, journalists, religious minorities, or politically exposed persons, and may endanger their relatives abroad. In the hands of criminals, it can be used to identify wealthy users and facilitate targeted extortion, including so-called "wrench attacks," in which physical violence or threats are used to coerce a victim into surrendering private keys or transferring funds.

The usual assumption is that PPSIs will collect this information, secure it, and use it responsibly. But once a database links identity records to blockchain addresses, it becomes a uniquely valuable honeypot. A breach would not simply expose static identifiers like in the traditional financial system, but also their linkage with a durable map of financial activity. That makes the breach risk more severe than in many traditional financial settings, where records are typically fragmented across institutions and are not automatically linked to a global, public, and immutable ledger.

This risk is avoidable. PPSIs should not be pushed toward compliance models that require them to build databases connecting real-world identities to public blockchain activity when less invasive alternatives can achieve the same or better AML/CFT outcomes. Privacy-preserving digital identity, portable credentials, attribute-based proofs, and risk-score attestations can allow PPSIs to verify relevant facts without retaining the raw materials for identity theft or creating a comprehensive identity-to-transaction map.

The constitutional concern is also substantial. If traditional BSA compliance is mechanically applied to PPSIs, the federal government may gain ready access to a customer's comprehensive blockchain activity without a warrant, subpoena, or probable cause. The issue is not merely that a customer provided onboarding information to a PPSI, but that linking that onboarding file to blockchain addresses may reveal a much broader record of peer-to-peer activity that the customer did not meaningfully disclose to the PPSI.[15] As in *Carpenter v. United States*, where the Supreme Court held that cell-phone users do not meaningfully assume the risk of exposing a comprehensive record of their physical movements merely by using a phone,[16] stablecoin users should not be treated as having voluntarily exposed a comprehensive dossier of their financial activities, beliefs, and associations merely because they transact on a public blockchain.

FinCEN should account for that Fourth Amendment concern before importing traditional BSA compliance expectations into the PPSI context. GENIUS requires PPSIs to maintain an effective customer identification program, including identification and verification of account holders, high-value transactions, and appropriate enhanced due diligence. But "effective" does not mean maximally invasive. It does not require PPSIs to collect and retain more sensitive information than necessary, nor does it require them to create identity-linked blockchain dossiers where privacy-preserving alternatives can produce equivalent or better compliance outputs. And with the operational risks in mind, traditional methods have not demonstrated meaningful effectiveness against cybercrime and fraud.

---

[15] Coin Ctr. et al. v. Yellen et al., Complaint ¶ __, at 29, https://coincenter.org/wp-content/uploads/2022/06/1-Complaint.pdf.
[16] *Carpenter v. United States*, 585 U.S. 296 (2018).

FinCEN should therefore expressly recognize privacy-preserving digital identity as an acceptable customer onboarding method for PPSIs. A modern CIP should allow PPSIs to verify the facts they need to know while minimizing the data they collect, the honeypots they create, and the risks they impose on lawful users. That approach would better serve AML/CFT goals while protecting the freedom, dignity, and security of everyday Americans.

3. Privacy-Preserving Digital Identity

FinCEN's 2024 *Financial Trend Analysis (FTA)* identifies three points in the identity process that can be exploited for illicit finance: validation, verification, and authentication.[17] These terms are drawn from NIST's Digital Identity Guidelines, most recently updated in July 2025. NIST defines them as follows:

- Validation: "The process or act of checking and confirming that the evidence and attributes supplied by an applicant are authentic, accurate, and associated with a real-life identity."[18]
- Verification: "The process or act of confirming that the applicant undergoing identity proofing holds the claimed real-life identity represented by the validated identity attributes and associated evidence."[19]
- Authentication: "The process by which a claimant proves possession and control of one or more authenticators bound to a subscriber account to demonstrate that they are the subscriber associated with that account."[20]

FinCEN identifies three corresponding modes of exploitation: impersonation, circumvention, and compromise.[21] These risks are amplified by the current BSA model, which generally requires financial institutions to independently collect, verify, and store extensive personal information about their customers. PPSIs are treated as financial institutions under the GENIUS Act and may be further defined as such under this proposed rule. If PPSIs are pushed into the same data-intensive identity model, they will inherit the same vulnerabilities: more databases

[17] Fin. Crimes Enf't Network, *Identity-Related Suspicious Activity: 2021 Threats and Trends*, FinCEN Financial Trend Analysis, Jan. 2024, at 3–6, https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf.
[18] *Supra* note 15, at 83.
[19] *Id*.
[20] *Id*. at 65.
[21] Fin. Crimes Enf't Network, *Identity-Related Suspicious Activity: 2021 Threats and Trends*, FinCEN Financial Trend Analysis, Jan. 2024, at 6–8, https://www.fincen.gov/system/files/shared/FTA_Identity_Final508.pdf.

of static identifiers, more opportunities for theft, and more reusable material for identity fraud and AML/CFT evasion.[22]

The customer identification process should therefore evolve to mitigate these risks and better protect Americans' sensitive information. Privacy-preserving digital identity tools can allow PPSIs to verify relevant facts about customers without collecting and retaining large stores of sensitive personal information. Properly designed, these tools can address the risks FinCEN identifies in validation, verification, and authentication while reducing the harms that flow from overcollection. For purposes of this proposed rule, FinCEN should expressly allow alternative onboarding methods that are portable, attribute-based, and dynamically risk-scored. Each component serves a distinct function.

a. Portable Onboarding

Portable onboarding allows customers to use digital identity credentials across multiple financial institutions, including PPSIs.[23] Today, each institution typically repeats the same onboarding process: collecting copies of identity documents, storing addresses and Social Security numbers, and maintaining its own silo of sensitive customer data. In the PPSI context, that approach would create a separate cyberattack target at each issuer.

Portable onboarding reduces that duplication. A customer who has already completed a high-assurance identity proofing process could present a verifiable digital credential (VDC) to a PPSI, rather than resubmitting the same sensitive documents. The PPSI would verify the credential's authenticity, status, and binding to the customer, without necessarily retaining the underlying identity evidence.

VDCs are cryptographically signed attestations about a person or entity. They may prove facts such as age, citizenship, verified account status, or successful completion of an identity proofing process.[24] The basic model involves an issuer, a holder, and a verifier. The issuer signs the credential using a private cryptographic key. The holder stores and presents the credential. The verifier checks the credential's integrity and authenticity using the issuer's corresponding public key.

Portable credentials should be designed to preserve privacy. Otherwise, they risk recreating the same identity-linked surveillance problems described above. Zero-knowledge proofs can allow a

---

[22] Peter Van Valkenburgh, *Comment of Coin Center on Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets*, Coin Ctr. (Oct. 20, 2025), https://coincenter.org/comment-of-coin-center-on-treasurys-request-for-comment-on-innovative-methods-to-detect-illicit-activity-involving-digital-assets/.
[23] *Id.*
[24] *Id.*

holder to prove that a credential supports a relevant fact without revealing the credential itself or the underlying personal information. Secure multi-party computation can allow multiple parties to compute a risk or eligibility result using private inputs without exposing those inputs to one another. In an onboarding or customer due diligence context, these tools could allow multiple institutions to contribute limited signals to a fraud or eligibility assessment without requiring any one PPSI to collect and store the full underlying data.

To maintain a high standard of implementation, FinCEN should look to NIST Identity Assurance Level 2 (IAL2) as a benchmark for portable onboarding. A PPSI that verifies a credential issued through an IAL2-compliant process, confirms its validity and revocation status, and authenticates the holder's control of the credential should be permitted to treat that process as satisfying relevant customer identification requirements.[25]

b. Attribute-Based Onboarding

FinCEN should also permit PPSIs to rely on attribute-based proofs rather than full identity disclosure where appropriate under the PPSI's risk assessment. Attribute-based onboarding allows a PPSI to verify the specific fact it needs to know, rather than collecting an entire identity dossier.

In many cases, a PPSI does not need to know every detail of a customer's identity to satisfy an AML/CFT objective. It may need to know that the customer has completed identity proofing at a specified assurance level, is not on a sanctions list, is located in an eligible jurisdiction, is not using a prohibited account type, or falls below a defined risk threshold. Those facts can be proven directly through credentials or derived proofs without requiring the PPSI to retain the customer's full identity documents and static identifiers.

This approach would reduce the honeypot risk described above. It would also better protect Americans from criminals who seek to steal and reuse their PII. Therefore, the compliance question should be whether the PPSI can produce reliable, auditable evidence that a relevant requirement was satisfied, not whether it has collected the maximum possible amount of personal information.

---

[25] "Under IAL2, the user's identity must be verified through validated documents and authoritative record checks, then cryptographically bound to a digital credential. The credential must also incorporate liveness and proof-of-possession controls to ensure that it is being used by the legitimate, live person who was originally proofed and not by a thief or an automated agent." Peter Van Valkenburgh, *Comment of Coin Center on Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets*, Coin Ctr. (Oct. 20, 2025), https://coincenter.org/comment-of-coin-center-on-treasurys-request-for-comment-on-innovative-methods-to-detect-illicit-activity-involving-digital-assets/.

One practical path would be a FinCEN-supervised pilot program. FinCEN could permit PPSIs to onboard a defined number of customers at low transaction thresholds using attribute-based proofs and data-minimized identity workflows. The pilot should test which facts are genuinely necessary for AML/CFT purposes, how those facts can be verified, and whether data-minimized onboarding produces equal or better outcomes than traditional document collection. FinCEN should issue a Request for Information (RFI) on how to structure such a pilot, including eligible attributes, assurance standards, audit requirements, transaction limits, and safe harbor conditions.

c. Dynamic Risk-Scoring

PPSIs will also be required to conduct ongoing CDD for their direct customers.[26] Dynamic risk-scoring could allow PPSIs to satisfy that obligation in a more privacy-preserving and adaptive way.

Today, customer risk scoring is generally internal, opaque, and data-intensive. Each institution collects personal information, monitors customer activity, and applies its own risk model. That approach encourages duplicative collection, makes scores non-portable, and leaves customers with little understanding of what facts matter or how to improve their standing.

A better approach would allow certain risk-scoring components to become standardized, widely understood, and reusable across the market. A customer could voluntarily subject themselves to a recognized risk-scoring process before engaging with any particular PPSI. That process could evaluate relevant attestations and signals, such as credential freshness, liveness checks, prior successful identity proofing, jurisdictional eligibility, wallet longevity, source-of-funds attestations, or non-appearance on sanctions or fraud lists. The customer could then present the resulting score or attestation to the PPSI they want to use, without necessarily revealing the underlying personal information that produced it.

The PPSI would receive a compliance output: for example, that the customer satisfies a defined low-risk onboarding threshold, falls within a permitted transaction tier, or requires enhanced due diligence. The underlying proofs, credentials, or inputs would remain private unless a higher-risk score, higher transaction threshold, or other legally relevant trigger required additional disclosure. This would preserve the risk-based structure of AML/CFT regulation

[26] *Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements*, 91 Fed. Reg. 18582, 18598 (proposed Apr. 10, 2026). https://www.govinfo.gov/content/pkg/FR-2026-04-10/pdf/2026-06963.pdf.

while reducing the need for every PPSI to independently collect and retain the same sensitive data.

An oracle, smart contract, or other neutral computation layer could aggregate multiple independent credentials and behavioral proofs into a portable score. Users would retain control over which credentials or attestations they submit to improve their score. PPSIs and regulators could audit the scoring logic, thresholds, and accepted inputs to determine whether the process reliably satisfies AML/CFT objectives. Open-source scoring methods, public criteria, and auditable parameters would help ensure that dynamic risk scoring does not become another opaque surveillance system.

Dynamic risk-scoring is not a substitute for CDD, but it could be a way to make CDD more precise, portable, and privacy-preserving. If implemented correctly, it would allow PPSIs to rely on well-understood risk outputs, update customer risk assessments as facts change, reduce dependence on static identifiers, and reserve intrusive data collection for cases where heightened diligence is actually warranted.

4. Demonstrable Outputs

FinCEN need not treat privacy-preserving digital identity as an abstract promise. PPSIs should be able to demonstrate whether alternative onboarding methods achieve AML/CFT objectives while reducing the risks created by excessive collection and retention of PII. Relevant outputs could include reduced identity-related suspicious activity, fewer incidents of identity-theft-enabled fraud, stronger assurance at onboarding, lower rates of account takeover, and fewer compromises of sensitive customer data.

These metrics should be evaluated over time. A PPSI that uses portable credentials, attribute-based proofs, or dynamic risk-scoring may not show system-wide effects immediately, especially if adoption is limited. But FinCEN can structure pilots, safe harbors, and reporting expectations to compare outcomes against traditional onboarding methods. The question should be practical: does the alternative method produce equal or better AML/CFT results while creating fewer cybersecurity, fraud, and privacy risks?

FinCEN should therefore study the use of privacy-preserving digital identity in regulated financial services, including PPSI onboarding. That study should assess whether data-minimized identity workflows reduce cybercrime, identity theft, account compromise, and fraud while maintaining or improving AML/CFT compliance outcomes. FinCEN could pair that study with a new FTA focused on identity-related suspicious activity, building on its 2024 FTA. Such an analysis should examine whether institutions using privacy-preserving identity tools experience different rates of identity-related suspicious activity, customer-data compromise,

account takeover, and fraud than institutions relying on traditional document collection and retention.

FinCEN need not bear the full cost of this evaluation. It could begin with a low-cost RFI, followed by a narrow pilot in which participating PPSIs submit anonymized and aggregated metrics as a condition of safe-harbor participation. Relevant metrics could include onboarding completion rates, identity-related suspicious activity, account takeover, identity-theft-enabled fraud, false positives, enhanced-due-diligence triggers, data-retention volumes, and incidents involving compromised customer information.

FinCEN could also coordinate with NIST—and particularly the National Cybersecurity Center of Excellence (NCCoE)—Treasury's innovation programs, academic researchers, and private standard-setting and civil liberties bodies[27] to evaluate the technical performance of privacy-preserving identity tools. FinCEN's role need not be to build or fund the infrastructure. It can define the AML/CFT questions, identify the compliance outputs it needs to see, and allow regulated participants and independent evaluators to generate the evidence. That approach would let FinCEN build a record for future guidance or rulemaking without creating a large new agency program.

To make that evidence possible, FinCEN should provide a clear pilot pathway and an appropriate safe harbor for PPSIs that deploy privacy-preserving identity tools in good faith, subject to defined controls, auditability, and reporting obligations. Without such protection, PPSIs will rationally default to legacy data collection, even where less invasive methods may better serve AML/CFT goals. With time, adoption, and measurable outputs, FinCEN can determine which methods actually reduce illicit finance risk, rather than assuming that more data collection means better compliance.

II. Secondary Market Activity and the Limits of PPSI Obligations

Coin Center supports FinCEN's clarification that a PPSI's intervention in secondary-market transactions should be triggered only by a lawful order, and that PPSIs are not required to monitor the secondary market or independently adjudicate whether particular secondary-market transfers should be blocked, frozen, or rejected.[28] That limitation is essential,

[27]Coin Center's John Hancock Project is one example of this kind of private-sector effort. The project is intended to convene technologists, civil-liberties advocates, academics, and regulated-market participants around privacy-preserving digital identity standards, including portable credentials, attribute-based proofs, and dynamic risk-scoring mechanisms. See Peter Van Valkenburgh & Ian Miers, *Tear Down This Walled Garden: American Values and Digital Identity* 4, Coin Ctr. (Sept. 18, 2025), https://coincenter.org/tear-down-this-walled-garden/.

[28] *Supra* note 26, at 18592.

because it helps preserve the distinction between a PPSI's direct customer relationships and the broader peer-to-peer activity that may occur after a stablecoin has entered circulation.

FinCEN asks how "a PPSI's AML/CFT program [should] account for risks on the secondary market?"[29] Coin Center believes the final rule should remain within the limits FinCEN has already recognized. PPSIs should not be turned into general-purpose monitors of secondary-market activity or private adjudicators of when to use technical freeze, burn, or transfer-restriction capabilities. Expanding PPSI obligations in that direction would impose heavy compliance burdens, create significant liability risk for wrongful intervention, and threaten the privacy and due process rights of lawful users.

FinCEN should therefore strengthen the final rule by making clear that secondary-market risk considerations do not create a duty to monitor all stablecoin transfers, surveil public blockchains, or independently determine whether a third-party transfer should be blocked. We understand that FinCEN does not intend to impose such obligations, but must work to ensure such obligations are not incidentally imposed from other obligations. PPSI obligations should remain tied to direct customer relationships, direct transaction roles, and lawful orders. As explained below, that approach is sound policy and necessary to keep PPSI obligations within constitutional bounds.

OFAC's proposal risks undermining that boundary. Coin Center recognizes that PPSIs, as U.S. persons, are subject to U.S. sanctions laws and may be required to block or reject prohibited transactions involving blocked persons or blocked property. Coin Center also recognizes that GENIUS requires PPSIs to implement a sanctions compliance program.[30] But OFAC's proposed rule appears to require PPSIs to identify "transactions that *may* violate or would violate U.S. sanctions" [emphases added] across stablecoin activity generally, including in the secondary market.[31] Read broadly, that requirement would pressure PPSIs to surveil public blockchains and make their own probabilistic judgments about which secondary-market transactions involve sanctioned persons or property.

Coin Center does not support expanding blockchain surveillance in this way. PPSIs should not be required to proactively determine, based on their own risk scoring or blockchain analytics, who should be blocked or whose funds should be frozen. OFAC should narrow its identification requirement to primary-market screening and direct customer activity, while allowing PPSIs to demonstrate targeted compliance capabilities when blocked persons or blocked property are

[29] *Id*. at 18620.
[30] *Guiding and Establishing National Innovation for U.S. Stablecoins Act*, Pub. L. No. 119-27, 139 Stat. 419 (2025), https://www.congress.gov/bill/119th-congress/senate-bill/1582/text.
[31] *Supra* note 26 at 18613.

identified in the secondary market by a lawful order or by a specific OFAC sanctions requirement. OFAC and FinCEN should also require procedural safeguards for any secondary-market blocking, freezing, or rejection capability, including safeguards against false positives and wrongful action against U.S. persons.

1. Constitutional Limits on Secondary-Market Freezes and Surveillance

The law has long distinguished between duties arising from a direct relationship and duties imposed toward the world at large. Anglo-American common law generally does not require a person to intervene in the affairs of strangers absent some special relationship, undertaking, agency, custody, control, or direct participation in the relevant conduct.[32] That principle is directly relevant to this rulemaking. A PPSI has legal obligations when it deals with its own customers, issues or redeems stablecoins, accepts a transmittal order, or responds to a lawful government command. A peer-to-peer transfer between third parties in the secondary market is different. The mere fact that the transferred instrument is a payment stablecoin issued by the PPSI should not create a free-floating duty to monitor, investigate, or interrupt transactions between persons with whom the PPSI has no privity, agency relationship, or direct transactional role.

That same distinction helps explain the private-nondelegation and due-process concerns raised by secondary-market intervention. The private-nondelegation doctrine rests on a simple constitutional premise: private parties do not hold the legislative or executive power of the United States, and government accountability is undermined when coercive public power is exercised by actors outside the constitutional chain of command.[33] Under the Eleventh Circuit's formulation, private-delegation concerns arise where the private actor does not function subordinately to an agency or where the agency does not retain adequate authority and

---

[32] See Restatement (Second) of Torts § 314 (Am. L. Inst. 1965) ("The fact that the actor realizes or should realize that action on his part is necessary for another's aid or protection does not of itself impose upon him a duty to take such action."); id. § 315 (no duty to control the conduct of a third person absent a special relationship with the third person or the person needing protection); id. § 314A (recognizing special relationships giving rise to duties to aid or protect); Restatement (Third) of Torts: Liability for Physical and Emotional Harm § 40(a) (Am. L. Inst. 2012) ("An actor in a special relationship with another owes the other a duty of reasonable care with regard to risks that arise within the scope of the relationship."); see also *DeShaney v. Winnebago Cnty. Dep't of Soc. Servs*., 489 U.S. 189, 195 (1989) ("[N]othing in the language of the Due Process Clause itself requires the State to protect the life, liberty, and property of its citizens against invasion by private actors.").

[33] See *Dep't of Transp. v. Ass'n of Am. R.Rs*., 575 U.S. 43, 62 (2015) (Alito, J., concurring) ("Private entities are not vested with 'legislative Powers.' Nor are they vested with the 'executive Power,' which belongs to the President."); *Carter v. Carter Coal Co*., 298 U.S. 238, 311 (1936) (describing delegation of coercive regulatory power to private parties whose interests may be adverse to others as "legislative delegation in its most obnoxious form").

surveillance over the actor's activities.[34] PPSIs may be required to screen their own customers, maintain sanctions controls, and respond to lawful orders. They should not be required to make binding, coercive determinations about third-party secondary-market users based on private blockchain analytics and without constitutionally adequate process or clear regulatory supervision and accountability.

Once the government pressures or requires a PPSI to monitor secondary-market transfers or freeze assets held by persons with whom the issuer may have no direct relationship, the issue is no longer ordinary customer-facing compliance. It is government-directed intervention against third parties. That move requires clear legal authorization and constitutional safeguards, especially where the intervention deprives a U.S. person of property or exposes a comprehensive record of lawful financial activity.

A stablecoin freeze implicates the Fourth Amendment because it interferes with property. A "seizure" occurs when the government meaningfully interferes with an individual's possessory interests in property.[35] A freeze of stablecoins does exactly that: it prevents the owner from using, transferring, redeeming, or otherwise exercising control over the asset. In *KindHearts for Charitable Humanitarian Development, Inc. v. Geithner*, a federal district court applied that principle to OFAC blocking and held that blocking an American organization's assets was a Fourth Amendment seizure.[36]

The Fourth Amendment reasonableness of such a seizure is especially doubtful where a PPSI freezes secondary-market assets based on probabilistic blockchain analytics rather than a warrant supported by probable cause. Address clustering, hop tracing, and other blockchain-forensics techniques may be useful investigative leads, but they do not establish that a particular U.S. person owns or controls a sanctioned address, transacted with a blocked person, or engaged in prohibited conduct. A rule that pressures PPSIs to freeze assets based on those inferences risks converting investigative suspicion into immediate deprivation of property. The Constitution does not permit the government to outsource that judgment to private issuers and analytics vendors, then leave innocent Americans to recover their property after the fact. At minimum, U.S. persons deserve a neutral arbiter, a lawful basis for restraint, and a meaningful opportunity to contest the deprivation.

---

[34] *Consumers' Research, Cause Based Commerce, Inc. v. FCC*, 88 F.4th 917, 925–26 (11th Cir. 2023); see also Brief for Petitioner at 23–29, *American Securities Association v. SEC*, No. 24-13751 (11th Cir. Feb. 27, 2025) (collecting authorities on private nondelegation and arguing that a nominally private regulator may not exercise legislative or executive power without adequate governmental supervision).

[35] *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

[36] *KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner*, 647 F. Supp. 2d 857, 904–08 (N.D. Ohio 2009).

The Fifth Amendment raises a separate due-process problem. Even where the government has authority to freeze property, the affected person must receive constitutionally adequate process. At minimum, due process requires fair notice of the basis for the deprivation and a meaningful opportunity to contest it before a neutral decisionmaker, subject to narrow exceptions for exigent circumstances.[37] In *KindHearts*, the same court that found an OFAC blocking order to be a seizure also held that OFAC violated the Fifth Amendment by failing to provide constitutionally adequate notice and a meaningful opportunity to respond.[38] If PPSIs are expected to freeze secondary-market assets first and leave affected users to seek relief later, lawful users may be deprived of property without knowing the evidence against them, without a timely path to contest the freeze, and without any prior judicial determination that their property is lawfully subject to seizure.

Secondary-market monitoring also raises a related Fourth Amendment concern. In *Carpenter*, the Supreme Court rejected the idea that individuals necessarily assume the risk of exposing a comprehensive digital record of their movements merely by using a cell phone.[39] Stablecoin users likewise should not be treated as having voluntarily exposed a comprehensive dossier of their financial activities, beliefs, and associations merely because they transact on a public blockchain. A rule that pressures PPSIs to link real-world identity data to secondary-market blockchain activity would risk creating precisely the kind of comprehensive digital record that demands constitutional caution.

These constitutional and common-law limits should guide the final rule. FinCEN should preserve the boundary between direct PPSI activity and secondary-market activity, and OFAC should not undermine that boundary by requiring PPSIs to surveil public blockchains or independently adjudicate suspected sanctions exposure. PPSIs may be required to respond to lawful orders and to maintain targeted technical capabilities. They should not be required to conduct generalized monitoring, make probabilistic seizure decisions, or freeze U.S. persons' property without constitutionally adequate process.

2. Customer Due Diligence

In the proposed rule, FinCEN states that PPSIs may need to consider public blockchain information to account for secondary market risks when conducting CDD.[40] It may be reasonable for a PPSI to consider relevant on-chain information when assessing the risk of a

[37] See *Mathews v. Eldridge*, 424 U.S. 319, 333–35 (1976).
[38] *Supra* note 36.
[39] *Carpenter v. United States*, 585 U.S. 296, 310–20 (2018).
[40] *Supra* note 26 at 18601.

direct customer. But that principle must be carefully limited. If read broadly, PPSIs may feel pressured to monitor every transaction their customers execute on a public blockchain in order to refine customer risk profiles. That would create serious privacy risks for customers and counterparties, and it would undermine FinCEN's stated intention not to impose secondary-market monitoring obligations.

CDD should not become a backdoor requirement for broad blockchain surveillance. PPSIs should not be expected to monitor downstream transfers merely because those transfers involve a payment stablecoin issued by the PPSI or interact with a PPSI-related smart contract. As explained above, PPSI obligations should remain tied to direct customer relationships, direct transaction roles, and lawful orders. The final rule should therefore clarify that customer due diligence obligations do not require PPSIs to build comprehensive transaction dossiers on customers or their counterparties in the secondary market.

FinCEN can preserve effective CDD without pushing PPSIs toward secondary-market surveillance. As discussed in the previous section, privacy-preserving identity tools can allow PPSIs to evaluate customer risk through portable credentials, attribute-based proofs, and dynamic risk scoring based on relevant behavioral attestations. Those tools can provide useful compliance outputs without requiring the PPSI to directly monitor customers' downstream transactions or identify their counterparties across public blockchains.

3. Recordkeeping Requirements

Coin Center does not object to FinCEN's treatment of PPSIs for recordkeeping purposes when a PPSI is actually accepting a transmittal order, including in connection with issuance, redemption, or other direct customer-account activity. But FinCEN should clarify that treating payment stablecoins as "money," "funds," or as included within the definition of a "transmittal order" does not convert secondary-market transfers into PPSI recordkeeping events.

A third-party transfer should not trigger PPSI recordkeeping obligations merely because it involves a payment stablecoin or interacts with a PPSI's smart contract. Existing recordkeeping obligations follow the regulated entity's direct role in a transaction, not the instrument being transferred. A bank does not keep records on every downstream cash transaction simply because it once issued or handled cash. Likewise, a PPSI should not become responsible for recording every secondary-market transfer of its stablecoin merely because the token moves on a public blockchain.

The text of 31 C.F.R. § 1010.410(e) supports this distinction. The rule focuses on whether a financial institution accepts a transmittal order as the transmitter's financial institution, an

intermediary financial institution, or the recipient's financial institution. Each role reflects direct involvement in the transfer of funds. FinCEN should apply the same logic here and clarify that third parties merely interacting with a PPSI's smart contract in the secondary market is not equivalent to the PPSI accepting a transmittal order.

The proposed rule already contains a similar clarification for suspicious activity reporting (SAR) obligations: "A transaction is not conducted or attempted by, at, or through a permitted payment stablecoin issuer only because a transfer by third parties results in an interaction with a permitted payment stablecoin issuer's smart contract."[41] FinCEN should adopt an analogous clarification for recordkeeping requirements and the Travel Rule.

Where recordkeeping requirements do apply, FinCEN should remain mindful of the operational risks described in the previous section. Recordkeeping rules can themselves create honeypots of sensitive customer data. If applied without considering data minimization, they may undermine the same cybersecurity, fraud-reduction, and privacy goals that FinCEN seeks to advance. FinCEN should therefore allow PPSIs to use privacy-preserving methods to satisfy recordkeeping obligations where legally sufficient.

For example, where a transaction triggers a recordkeeping, reporting, information-sharing, or other compliance obligation, a PPSI could use privacy-preserving methods to preserve or transmit required information without broadly exposing sensitive personal data by default. ZKPs and related tools may allow a PPSI to prove that required information exists, is complete and valid, and is bound to the relevant transaction, while keeping the underlying information encrypted or otherwise shielded unless disclosure is legally required. FinCEN should expressly invite development of these architectures, for example a "zero-knowledge Travel Rule": a framework in which required originator and beneficiary information remains private in ordinary operation, but can be verified, transmitted through the relevant chain of regulated financial institutions, or disclosed to appropriate parties under the conditions required by law.

4. OFAC Sanctions Obligations

Coin Center recognizes that PPSIs, as U.S. persons, are subject to U.S. sanctions laws and may be required to block or reject prohibited transactions from blocked persons. Coin Center also recognizes that GENIUS explicitly requires PPSIs to create and maintain a sanctions compliance program.[42] But that requirement should not be interpreted to impose mass surveillance obligations over public blockchains or to require PPSIs to make independent freezing decisions based on probabilistic blockchain analytics.

---

[41] *Supra* note 26 at 18608.
[42] *Supra* note 30.

GENIUS requires that a sanctions compliance program be tailored to the PPSI, consistent with applicable law, be reasonably designed, and include verification of sanctions lists.[43] OFAC should not interpret that language to authorize deputizing PPSIs as general-purpose blockchain monitors. Nor should OFAC require PPSIs to seize or freeze property based on their own probabilistic judgments about whether a secondary-market transfer may involve a sanctioned person or prohibited transaction.

Such an approach would create the constitutional problems described above. If PPSIs are required to identify potentially prohibited transactions across all secondary-market activity involving their stablecoins, they cannot comply without first surveying large volumes of public blockchain activity, including activity by U.S. persons. That surveillance would be undertaken at the government's direction and for the government's enforcement purposes, and it would therefore raise serious Fourth Amendment concerns.

The seizure risk is equally serious. A PPSI attempting to comply with a broad identification requirement may mistakenly freeze the assets of U.S. persons based on imperfect analytics. Common blockchain analytics techniques, including tracing through "hops" and address clustering, rely on probabilistic inferences. They can be useful investigative tools, but they do not establish with certainty that a particular person owns, controls, or benefits from a particular address. If OFAC requires PPSIs to act on those inferences, lawful users may be deprived of property without adequate process.

For these reasons, OFAC should limit PPSI sanctions obligations to primary-market screening, direct customer activity, and targeted secondary-market action when blocked persons or blocked property are identified by a lawful order or by a specific OFAC sanctions requirement. PPSIs should be able to demonstrate that they possess targeted compliance capabilities, but they should not be required to act as monitors and independent adjudicators of the secondary market.

OFAC and FinCEN should also require procedural safeguards for any secondary-market blocking, freezing, or rejection capability. Those safeguards should include mechanisms to reduce false positives, promptly notify affected persons where legally permissible, provide a meaningful path to contest mistaken freezes, and protect U.S. persons from warrantless or unsupported deprivation of property. Sanctions compliance is important, but it must remain bounded by constitutional limits, the common-law distinction between direct obligations and duties to strangers, and basic due process.

---

[43] *Id.*

OFAC and FinCEN should not assume that false positives in this context would be minor compliance errors. A miscalibrated secondary-market dragnet could deprive innocent Americans of property, expose their lawful financial activity, and leave them with no meaningful way to clear their names. Coin Center has brought constitutional challenges before when federal financial-surveillance mandates exceeded lawful bounds, and it would view any regime that predictably freezes U.S. persons' stablecoins based on probabilistic analytics and administrative pressure as presenting grave Fourth and Fifth Amendment concerns. OFAC should not force innocent Americans, or the organizations that defend them, to vindicate those rights in court.

III. Conclusion

Payment stablecoins can provide freer, faster, and more open forms of payment, but only if the rules are carefully tailored to avoid identity-linked financial surveillance and remain consistent with the U.S. Constitution. This tailoring does not have to undermine AML/CFT efforts. Digital identity solutions are evolving to be privacy-preserving, and allowing PPSIs to adopt alternative onboarding methods would mitigate operational risks and provide everyday Americans with greater security, while still complying with AML/CFT obligations.

Thus, FinCEN should recognize that overcollection of sensitive customer information can increase cybercrime, fraud, and downstream money laundering risks. In response, FinCEN should expressly permit PPSIs to use privacy-preserving digital identity tools where they produce auditable compliance outputs and minimize data collection from direct customer onboarding.

FinCEN and OFAC should also preserve the boundary between primary-market PPSI activity and secondary-market peer-to-peer transfers. PPSIs should, of course, screen their own customers, maintain lawful compliance programs, and respond to lawful orders. However, these obligations should not go so far as to require public blockchain surveillance or the construction of identity-linked transaction dossiers, nor require PPSIs to independently adjudicate and freeze assets based on probabilistic analysis. The Fourth and Fifth Amendments should guide FinCEN and OFAC in avoiding warrantless surveillance and the deprivation of Americans' property without due process.

Sincerely,

Lizandro Pieper
Research Director of Coin Center