Comment of Coin Center to FinCEN and the Agencies on Permitted Payment Stablecoin Issuer Customer Identification Program

August 21, 2026
RIN 1506–AB74

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), Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) (collectively, the "Agencies") for the opportunity to comment on *Permitted Payment Stablecoin Issuer Customer Identification Program* pursuant to the *GENIUS Act*.

GENIUS requires a permitted payment stablecoin issuer (PPSI) to maintain an "effective" customer identification program (CIP), which would include "identification and verification of account holders."[1] Understandably, the Agencies' proposal reflects a continuation of existing CIP requirements for financial institutions—as no alternative yet exists for financial institutions. But traditional customer identification and verification have proven ineffective and even risky for both customers and financial institutions, as maintaining massive datasets of sensitive personal information has proven vulnerable to illicit actors and foreign adversaries—all to comply with federal regulations. Given new technological advances, PPSIs present a novel opportunity to depart from the status quo and introduce methods for customer verification that preserve privacy and provide autonomy while ensuring effective compliance.

[1] 12 U.S.C. § 5903(a)(5)–(6) (Supp. I 2025). https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title12-section5903.

In past comment letters to the Department of Treasury, and specifically FinCEN and OFAC, Coin Center has proposed permitting these technologies for PPSIs because of the potential for user-controlled digital identity (UCDI) solutions that are decentralized and privacy-preserving.[2] We have also requested that FinCEN allow for PPSIs to issue stablecoins on privacy-preserving blockchains,[3] while, of course, leveraging UCDI to maintain compliance with the law. We would like to thank the Agencies for broadly considering innovative methods for CIP.[4] However, these technologies must be properly designed to provide customers with greater agency and privacy; otherwise, we risk unprecedented mass surveillance and honeypots of sensitive data ripe for attacks. The very risks that exist with traditional CIPs would continue or worsen, while imposing greater limits on American values of privacy and speech.

The first section summarizes our past responses to Treasury and FinCEN. We then turn to the risks of designing digital identity and verifiable credentials without proper protections. These risks present grave consequences of which the Agencies must be aware.

Lastly, we address specific matters concerning customer relationships in the proposed rule. This section is split into three parts. First, we suggest for the final rule to replace "formal relationships" with "contractual relationships" in the definition for "accounts," and to explicitly outline operational elements to make such relationships legally enforceable. This would draw a clear and necessary distinction between the primary and secondary markets. Second, we oppose applying CIP requirements for secondary market transactions. Doing so would impose unprecedented blockchain surveillance, create privacy risks for users, jeopardize regulatory objectives concerning illicit finance, and raise constitutional concerns. Third, we suggest leveraging privacy-preserving technologies for customer verification when the only interaction between a PPSI and user is redemption of stablecoins, because requiring a PPSI to collect and retain a redeemer's information for this isolated interaction would be unnecessary and risky.

I. Past Responses Concerning Permitted Payment Stablecoin Issuers' GENIUS Obligations

[2] Coin Center, *Comment of Coin Center on Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets* (Oct. 17, 2025). https://coincenter.org/wp-content/uploads/2025/10/Comment-of-Coin-Center-on-Treasurys-Request-for-Comment-on-Innovative-Methods-to-Detect-Illicit-Activity-Involving-Digital-Assets.pdf; Coin Center, *Comment of Coin Center to FinCEN and OFAC on PPSI AML/CFT and Sanctions Program Requirements* (June 9, 2026). https://coincenter.org/wp-content/uploads/2026/06/2026-06-09-FinCEN_OFAC-PPSI-NPRM-Response-Final.pdf

[3] Coin Center, *Innovative Methods*, supra note 2, at 5–8.

[4] *Permitted Payment Stablecoin Issuer Customer Identification Program*, 91 Fed. Reg. 37,234, 37,242 (proposed June 22, 2026). https://www.govinfo.gov/content/pkg/FR-2026-06-22/pdf/2026-12460.pdf.

The central thesis of our previous two responses is that financial regulations should only require verifiable compliance outcomes from PPSIs, rather than maximal collection, retention, and linkage of personal information. Open, user-controlled, privacy-preserving technologies can establish the facts regulators need to accomplish their objectives, while avoiding centralized identity databases, permanent financial dossiers, and surveillance of stablecoin users. This thesis is equally applicable to the CIP requirements discussed in this proposed rulemaking by the Agencies. Therefore, we will go over past responses before transitioning to direct application to the Agencies' proposed CIP rule.

1. Technical Components for User-Controlled Digital Identity

The solutions we describe were first developed in Coin Center's report *Tear Down This Walled Garden*—which began the initiative known as the John Hancock Project—where we advocated for replacing the existing identity verification framework that is "costly, privacy-invasive, and ineffective at deterring illicit finance" with portable, user-controlled verifiable credentials.[5] This framework consists of four technical components: verifiable digital credentials (VDCs), zero-knowledge proofs (ZKPs), multi-party computation (MPC), and open blockchain networks.

VDCs are "cryptographically signed digital document[s] that prove[] something about you—such as your age, citizenship, or verified account status."[6] These can be designed such that "a verifier can check the credential's provenance without calling back to the original issuer"[7] by using ZKPs and MPC. A ZKP mathematically proves something without revealing the underlying information.[8] Similarly, MPC allows multiple independent parties to contribute private information without exposing it to each other—such as a "risk rating" from a bank.[9] Together, these two components allow a VDC to prove private inputs stemming from multiple independent parties.

This is where an open blockchain network can serve as a neutral coordination layer and verification infrastructure. In order for this framework to function properly, there needs to be an underlying infrastructure for coordinating information and verification. We do not want said coordinator to be a centralized intermediary that acts as the gatekeeper and arbiter of trust. Such a system would inevitably recreate the very issues we wish to depart from in the

---

[5] Peter Van Valkenburgh & Ian Miers, *Tear Down This Walled Garden: American Values and Digital Identity* 1 (Coin Center, Sept. 2025). https://coincenter.org/tear-down-this-walled-garden/
[6] *Id*. at 12.
[7] *Id*.
[8] *Id*. at 15.
[9] *Id*.

traditional identification system—that is, mass surveillance and control.[10] Such an intermediary would be able to decide who can or cannot participate, what technologies can or cannot be used (likely favoring its own), and how it wishes to handle sensitive information.[11] For that reason, we need an open system that anyone can participate in, is auditable, and is decentralized. Here, VDCs can remain portable and interoperable across institutions, because they "can be issued, combined, verified, and revoked according to shared, transparent rules—without a central gatekeeper."[12]

This infrastructure also allows for dynamic risk scoring:

> "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."[13]

2. Permitting Adoption of Privacy-Preserving Technologies by Permitted Payment Stablecoin Issuers

These four technical components make up the greater framework for UCDI that can be leveraged in cases like direct customer services provided by PPSIs. Coin Center's two comments pursuant to GENIUS' rulemakings took the framework from our report and presented it to Treasury and FinCEN as an innovative method for anti-money laundering and countering the financing of terrorism (AML/CFT) while protecting stablecoin customers from the perils of traditional identification schemes—more commonly known as know-your-customer, or KYC.

---

[10] *Id*. at 17.
[11] *Id*.
[12] *Id*.
[13] Coin Center, *PPSI AML/CFT,* supra note 2, at 11.

Coin Center first made the case for UCDI to Treasury in our October 2025 response to its *Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets*. We began by first examining the flaws of current customer identification approaches—mainly, that they are "costly, privacy-invasive, and ineffective at deterring illicit finance."[14] Considering that "U.S. financial institutions spend roughly $26 billion annually on AML and sanctions compliance," and $300 billion globally, AML regulatory regimes, like the Bank Secrecy Act (BSA), only intercept and recover 0.2 percent of criminal proceeds.[15] These results are staggering, especially since the current system harms law abiding citizens by exposing them to cybercriminals who attempt to steal their data and their identities.[16]

Coin Center took an even deeper dive into these security risks in our June 2026 response to FinCEN and OFAC's *Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements*. We examined how illicit actors are more empowered to commit cybercrimes and fraud when financial institutions must collect and retain sensitive customer information.[17] AML/CFT efforts are also compromised here, because, as FinCEN identified, illicit actors exploit the identity process at financial institutions by "impersonating others, exploiting insufficient processes to circumvent verification, and using compromised credentials to gain unauthorized access to accounts."[18] In fact, in addition to FinCEN, the Federal Bureau of Investigation, the Federal Trade Commission, and the National Institute of Standards and Technology have all reported massive amounts of cybercrime and fraud that harm both customers and financial institutions, all stemming from obligated KYC.[19] In other words, KYC itself creates an AML/CFT risk.

For this reason, in both responses, Coin Center requested that FinCEN allow PPSIs to adopt innovative methods for customer verification and AML/CFT obligations that preserve customer privacy. Wee advocated for permitting the use of UCDI in direct customer onboarding by PPSIs, as well as for the ability to issue stablecoins on privacy-preserving blockchains. Specifically, we stated:

> "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.

---

[14] Coin Center, *Innovative Methods*, supra note 2, at 1.
[15] *Id*. at 2.
[16] *Id*. at 3.
[17] Coin Center, *PPSI AML/CFT,* supra note 2, at 3-6.
[18] *Id*. at 5.
[19] *Id*. at 4-5.

> 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."[20]

The use of UCDI would mitigate these risks, especially when combined with a privacy-preserving blockchain. But beyond that, these technologies do not just protect against illicit actors, they also empower Americans with the authority to decide which information they wish to disclose and which information they wish to protect. Privacy is a means for security and agency in one's dealings. As we argued in our previous responses, blockchains are often designed to show all the details of every transaction ever made and the balance of each wallet. In the event that an illicit actor or hostile government—foreign or domestic—links an identity to a wallet address, then the owner of the wallet will have their complete financial history exposed. This is problematic:

> "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."[21]

Thus, privacy is a means for security. It provides the user with greater authority over their sensitive information (e.g., their PII, wallet balance, and transaction history), allowing them to

[20] *Id*. at 3.
[21] *Id*. at 6.

decide which information to disclose and which to protect. UCDI and privacy-preserving blockchains can manifest this authority for stablecoin transactions, while providing PPSIs with the proper tools to maintain regulatory compliance.

PPSIs have certain regulatory obligations they must meet to ensure that they are preventing fraud and illicit finance, and their customers must abide by those obligations to use their services, but these obligations do not warrant the overcollection of information to fulfill their objectives. PPSIs merely need proof that direct customers are who they say they are, and the technology to do so exists and is quickly improving. Coin Center has made this recommendation to FinCEN, and the Agencies should follow suit. We will discuss the matter in more detail in the next section.

II. Considerations for Digital Identity and Verifiable Digital Credentials in Customer Identification Programs

We appreciate the Agencies' flexibility in considering innovative methods for CIP requirements. The Agencies recognize the advancements made in digital identity and VDCs as a means for customer verification, but are rightfully concerned with "how they operate and in their trustworthiness."[22] While existing customer onboarding itself is risky and ineffective, institutions should not be so quick to adopt just any developing technologies.

Depending on how digital identity solutions and VDCs are designed, the benefits can be substantial for financial institutions and regulatory regimes to achieve their objectives and protect against various risks to both financial institutions and their customers. If poorly designed, they can expose financial institutions and customers to unprecedented risks, and undermine regulatory objectives. Therefore, these technologies must be designed to be open, decentralized, and privacy-preserving.

Without a privacy-preserving design, digital identity links a person's identity to their digital footprint and provides a complete dossier of all their doings. This is especially problematic with a blockchain that makes navigating this information more intuitive and the details more expansive. Additionally, in the event that these technologies are centralized, honeypots of sensitive information will still exist in the same way that they exist with legacy CIP. Nothing is solved here, but the risks grow substantially for customers. Identity management systems that rely on centralized infrastructure have always been at risk of hacks for sensitive customer

[22] *Permitted Payment Stablecoin Issuer Customer Identification Program*, 91 Fed. Reg. 37,234, 37,242 (proposed June 22, 2026). https://www.govinfo.gov/content/pkg/FR-2026-06-22/pdf/2026-12460.pdf.

information. That information can be weaponized by hostile foreign adversaries,criminals, or even corrupt government agents. As Coin Center previously counseled:

> "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."[23]

As previously explained, digital identity can be designed and built in a way that provides a person with more sovereignty over their sensitive information while allowing financial institutions to comply with the law and reduce operational risks.[24] With greater privacy, a person can be less exposed to identity theft, fraud, and other forms of crime, such as extortion.[25] They are also freer to be themselves, including by contributing to political causes or religious institutions that may otherwise lead to discrimination if publicly disclosed.

Additionally, a digital identity solution that depends on portable, user-controlled identity credentials or attribute proofs that can be issued once and reused across regulated relationships would be more secure and accomplish customer verification. This approach, consistent with Coin Center's previous response to FinCEN and the John Hancock Project, would reduce repeated collection of sensitive personal information while preserving verifiable compliance with AML/CFT obligations.

There is no reason we cannot build a privacy-preserving and effective regulatory system, with customers foremost in mind. The Agencies should not treat VDCs merely as a supplement after a PPSI has collected traditional customer information. A properly designed system can allow a PPSI to satisfy customer identification and verification objectives without collecting, copying, and retaining underlying identity documents, static identifiers, or full identity dossiers. Stated differently, PPSIs do not need to collect old forms of documentation when a person can mathematically prove (via software) that they are who they say they are and that they maintain the attributes necessary to comply with the law (e.g., they are not sanctioned).

---

[23] Coin Center, *PPSI AML/CFT,* supra note 2, at 7.
[24] *Id*. at 2-8.
[25] *Id*. at 6.

However, despite these advancements, the proposed rule only considers these technologies as supplementary methods to the existing CIP requirements. This would ultimately defeat the purpose of privacy-preserving technology if PPSIs were still required to collect and retain documentation containing sensitive personal information. At minimum, a PPSI should be able to use a VDC to verify required identifiers without collecting source documents, the complete credential, or unrelated attributes.

The final rule should therefore clarify that a PPSI may use a UCDI or comparable privacy-preserving digital identity proof as a primary method of customer identification and verification, not merely as a supplemental method. The PPSI should not be required to collect or retain the underlying identity document or all underlying personal information where an alternative method accomplishes the same regulatory outcome. Furthermore, the Agencies should consider a pilot, safe harbor, or other legal framework under which verified attributes can substitute for collecting and retaining static identifiers.

Relatedly, the final rule should recognize that obligations to cross-reference "government lists"[26] can be satisfied through these same data-minimized methods upon onboarding a customer. Treasury and the relevant regulators have not yet designated any such lists for purposes of this provision, therefore, the rule should preserve flexibility so that future list-screening directives can be implemented through VDCs, attribute-based proofs, or other privacy-preserving methods.

III. Customer Relationships

The Agencies consider various customer relationship circumstances in the proposed rule that we also wish to address. First, whether "formal relationship" should be included in the definition for "account."[27] Second, whether or not CIP requirements should extend to secondary market activities.[28] Third, whether the final rule should account for situations where a customer's only desired relationship with a PPSI is for stablecoin redemption.[29]

We support the Agencies' recognition that purely secondary-market payment stablecoin activity (i.e., activity that does not directly involve the PPSI as a party to the transaction other than via a smart contract) would not establish a formal relationship or create an "account." We

[26] *Supra* note 22 at 37243.
[27] *Id.*
[28] *Id.* at 37244.
[29] *Id.*

also support the clarification that mere ownership or control of a PPSI's payment stablecoin, without additional evidence of a direct relationship with a PPSI, does not constitute an account.

As Coin Center has emphasized in our previous response to FinCEN, AML/CFT obligations concerning customer verification should remain with the primary market, because identifying every third-party that exists in the secondary market creates privacy and constitutional concerns.[30] Therefore, for these considerations, the Agencies should continue to adhere to its principle by closing any gaps that could potentially include the secondary market into CIP requirements. This means replacing "formal relationship" with a more precise term; refraining from extending CIP requirements to secondary market activity; and treating redemption-only transactions with a PPSI as isolated events that do not constitute an "account."

1. Replacing "Formal Relationship" with "Contractual Relationship" in the Definition of an "Account"

The Agencies should start by replacing "formal relationship" with the more precise term of "contractual relationship." "Contractual relationship" provides the clearest boundary because it is derived from the ordinary legal meaning of "contract"—which already has certain requirements that resonate with a direct customer relationship. This definition would also be consistent with the existing definition of an "account" under current mutual fund CIP regulations,[31] but with some modifications.

Specifically, for our purposes, the Agencies should omit "other business relationships" that is currently included in the mutual fund definition for "account" in order to avoid ambiguity. Using "business relationship" would not solve the lack of clarity that "formal relationship" already introduces, while "contractual relationship" does. This sentiment was shared by federal agencies when finalizing the bank CIP rule, where "business relationship" was dropped from the definition for "account" in order to distinguish financial products and services from general business dealings.[32] The Agencies should not make the mistake of including it for PPSIs, where "contractual relationship" would do the necessary work for clear regulations.

---

[30] Coin Center, *PPSI AML/CFT,* supra note 2, at 13-21.

[31] 31 C.F.R. § 1024.100 (2026). https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1024/subpart-A/section-1024.100.

[32] "First, the reference to the term 'business relationship' has been deleted from the definition of 'account.' This change is made to clarify that the regulation applies to the bank's provision of financial products and services, as opposed to general 'business' dealings, such as those in connection with the bank's own operations or premises." See: *Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks*, 68 Fed. Reg. 25,090, 25,092 (May 9, 2003). https://www.govinfo.gov/content/pkg/FR-2003-05-09/pdf/03-11019.pdf#page=3

A contract requires the following elements to make it legally enforceable: "mutual assent (offer and acceptance), consideration (something of value is exchanged), capacity (e.g., minimum age, sound mind), and legality (lawful purpose)."[33] It is important that the Agencies make these principles operational for an account by requiring: a clear notice of PPSI service terms; objective and affirmative manifestation of assent; acceptance of the person's request for a service provided by the PPSI; and reciprocal, enforceable obligations concerning an issuer-provided service. These proposed requirements build upon existing GENIUS requirements for issuer disclosure and redemption obligations,[34] the difference here being an affirmative agreement being made between PPSI and a particular customer.

With a switch to "contractual relationship," combined with our proposed operational elements, the term "account" should provide the legal clarity necessary to maintain the boundary between direct customers and the secondary market.

2. Customer Identification Program Requirements Should Not Extend to Secondary Market Activity

Relatedly, with regards to the Agencies' considerations for secondary market CIP requirements, there is no question that duties arise when a PPSI deals with a direct customer, but requiring identification of all downstream users would be inconsistent with the American tradition of common law, where a person is not generally required to "intervene in the affairs of strangers absent some special relationship, undertaking, agency, custody, control, or direct participation in the relevant conduct."[35] Such an expansion of CIP requirements would impose unprecedented blockchain surveillance, creating privacy risks for users and jeopardizing

---

[33] *Contract*, Wex, Legal Information Institute, Cornell Law School (last reviewed Oct. 2025). https://www.law.cornell.edu/wex/contract.

[34] See: 12 U.S.C. § 5903(a)(1)(B)(i)–(ii) (requiring public disclosure of clear and conspicuous procedures for timely redemption and plain-language disclosure of purchase and redemption fees); id. § 5901(22)(A)(ii)(I) (defining a payment stablecoin partly through the issuer's obligation to convert, redeem, or repurchase it for a fixed amount of monetary value); id. § 5903(a)(5)(A)(v) (requiring identification and verification of "account holders with" a PPSI); see also id. § 5903(a)(7)(A)(i)–(v) (identifying issuance, redemption, custody, and related issuer-provided services). These provisions establish issuer-side disclosures and obligations but do not specify the affirmative agreement through which a particular holder becomes a direct customer of the PPSI. https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title12-section5903, and https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title12-section5901.

[35] Coin Center, *PPSI AML/CFT,* supra note 2, at 15.

regulatory objectives—as we have witnessed with the current regime's failures to prevent fraud and illicit finance.

From a constitutional perspective, such an expansion would also raise Fourth Amendment concerns:

> "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. 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."[36]

3. Redemption-Only Transactions Should Not Constitute Accounts

In the event a user decides to redeem a stablecoin directly from the PPSI, it would be risky to require the collection and retention of sensitive personal information for such an isolated event. This is a narrow transaction that is not the same as having an ongoing account with the issuer, and therefore, should not constitute opening an account. Requiring a PPSI to collect and retain a redeemer's information for this isolated interaction would be unnecessary, when the PPSI should be permitted to rely on proofs of the specific facts legally necessary to process the redemption, such as eligibility and applicable sanctions or government-list status.

This is where privacy-preserving proofs would be useful, allowing the redeemer to establish the specific facts necessary for the PPSI to determine that it may lawfully complete the redemption without unnecessarily linking an identity with a wallet address. Therefore, the Agencies should explicitly exclude redemption-only transactions from constituting an "account," and clarify that said transactions may be satisfied through privacy-preserving proofs and attestations.

IV. Conclusion

The collection and retention of customer information for CIPs is a risk in and of itself. As we have explained, the status quo is neither safe nor effective, and continuing its imposition to evolving technologies and financial landscapes will prove detrimental to Americans. The

[36] *Id*. at 17.

Agencies should avoid this outcome by permitting the adoption of privacy-preserving digital identity (i.e., UCDI) and stablecoin issuance on privacy-preserving blockchains. Doing so would not jeopardize regulatory objectives to combat illicit finance and fraud, but rather, empower them.

Additionally, CIP requirements should not bleed into secondary market transactions where there is no contractual relationship between PPSI and user. And in the event the only interaction is for redemption, then PPSIs should be permitted to rely on privacy-preserving proofs to establish the necessary facts for compliance without exposing users to risks inherent in CIPs.

By following these recommendations, the Agencies will better protect PPSIs' customers and strengthen efforts to reach their regulatory objectives. Maintaining the status quo, on the other hand, will undoubtedly undermine these efforts and place PPSIs and their customers at risk. If it is true that the Agencies wish to prevent illicit finance and fraud, they must choose the former; choosing the latter signals that these objectives are secondary to maintaining mass surveillance, and that is not a path the United States should follow.

Sincerely,

Lizandro Pieper
Research Director at Coin Center