the Solari Report

Catherine Austin Fitts, President
P.O. Box 157
Hickory Valley, Tennessee 38042
solari.com | info@solari.com

June 9, 2026

Regulatory and Strategic Affairs Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Assistant Director for Regulatory Affairs
Office of Foreign Assets Control
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW

Re: Comments on Notice of Proposed Rulemaking — Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, **Docket No. FINCEN-2026-0100; RIN 1506-AB73; 91 FR 18582 (April 10, 2026)**

Dear Regulatory Affairs Officials:

Solari, Inc. submits these comments in response to the joint Notice of Proposed Rulemaking (the "Proposed Rule") issued on April 8, 2026 by the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC") (collectively, "Treasury"), implementing provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (the "GENIUS Act"). The Proposed Rule, published in the Federal Register on April 10, 2026 at 91 FR 18582, would establish a new Anti-Money Laundering/Countering the Financing of Terrorism ("AML/CFT") program framework and economic sanctions compliance program requirements for permitted payment stablecoin issuers ("PPSIs") under new 31 C.F.R. Part 1033 and 31 C.F.R. Part 502, respectively.

Solari, Inc. is the publisher of the Solari Report (www.solari.com), a subscription service whose mission is to support individuals, families, and communities in building financial sovereignty, privacy, and resilience. Our subscribers and clients include individuals across the economic spectrum who rely on the integrity and accessibility of the U.S. payments system. We write in support of a payments

system that is safe, transparent, accessible, and free from discriminatory or politically motivated controls on access to financial services.

We recognize that the GENIUS Act establishes important obligations for PPSIs and that the financial integrity concerns animating the Proposed Rule are genuine and serious. The illicit finance risks associated with stablecoins — including their documented use in money laundering, sanctions evasion, terrorist financing, and narcotics trafficking — are well-evidenced and demand a rigorous regulatory response. We write not to diminish the importance of BSA and OFAC compliance in the stablecoin ecosystem, but to urge Treasury to structure that compliance framework in a manner that (1) protects the financial privacy rights of law-abiding consumers; (2) prevents the infrastructure of compliance from being weaponized as a tool of viewpoint discrimination or social control; and (3) safeguards due process rights when freezes, blocks, and transaction denials are implemented. We respectfully urge Treasury to strengthen the Proposed Rule in the specific respects set forth below.

I. THE TECHNICAL CAPABILITY TO BLOCK, FREEZE, AND REJECT TRANSACTIONS MUST BE SUBJECT TO ROBUST DUE PROCESS PROTECTIONS AND PROHIBITION OF VIEWPOINT-BASED DISCRIMINATION

Proposed § 1033.240 would require PPSIs to maintain technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions and to comply with the terms of any "lawful order." We support the obligation to maintain these technical capabilities as necessary for effective sanctions compliance and GENIUS Act implementation. However, the Proposed Rule is entirely silent on the due process framework that should govern the exercise of these capabilities, and on the critical question of whether those capabilities may be exercised for reasons unrelated to legal compliance obligations. This silence creates serious risks that must be addressed in the final rule.

A. The Proposed Rule Must Establish a Due Process Framework for Freezes and Blocks

Unlike a traditional bank account block or freeze, which requires a documented legal basis and is subject to regulatory and judicial review, a smart-contract-implemented block or freeze can be executed automatically and instantaneously without any contemporaneous human decision. The GENIUS Act requires PPSIs to have the capability to block and freeze; it does not eliminate the legal process requirements that ordinarily attend such actions. Treasury should therefore amend the Proposed Rule to require that:

- Any freeze, block, or suspension of a customer's payment stablecoin holdings or transaction capabilities that is not implemented pursuant to (a) a valid OFAC blocking order under applicable sanctions programs, (b) a specific court order, (c) a specific administrative order issued under applicable law and subject to judicial review, or (d) an AML-related hold pending SAR completion consistent with applicable guidance, must be accompanied by prompt written

notice to the affected customer identifying the legal basis for the action and the available process for challenging it.

- Treasury should publish examination guidance confirming that PPSIs may not use their block/freeze technical capabilities to restrict customer access based on factors unrelated to legal compliance obligations, including a customer's lawful purchasing behavior, political speech, industry affiliation (where lawful), or any other characteristic or activity not identified as a compliance trigger under applicable law or regulation.
- Treasury should make explicit in the preamble that the term "lawful order" as defined in proposed § 1010.100(rrr) does not authorize Treasury, FinCEN, or any other federal agency to direct PPSIs to implement class-wide blocks or freezes affecting categories of customers based on viewpoint, industry, location, legal conduct, health or citizenship status, or political or religious affiliation, absent specific statutory authorization.

B. PPSIs Must Be Prohibited from Discriminatory Use of Block and Freeze Capabilities

The documented history of financial debanking in the United States — including the well-documented targeting of firearms dealers, fossil fuel companies, cannabis businesses, and political and alternative health advocacy organizations through financial access restrictions — demonstrates that financial infrastructure can and will be deployed as a tool of viewpoint-based discrimination when regulatory frameworks do not affirmatively prohibit it. Programmable payment stablecoins amplify this risk: a smart-contract-implemented block can be executed at scale, automatically, without any human decision-maker and potentially without any notice to the affected customer or effective ability for the customer to protest improper or mistaken action.

Treasury should amend the Proposed Rule to expressly prohibit any PPSI from blocking, freezing, suspending, or terminating a customer's access to payment stablecoin services, or from declining to process any specific transaction, whether directly or through the operation of any smart contract, algorithm, or automated decision system, based on:

- Political opinion, political affiliation, or political speech, including support for or opposition to any candidate, party, policy, legislation, or governmental action;
- Religious beliefs, religious exercise, or religious affiliation;
- Race, ethnicity, national origin, disability, sex or sexual orientation, age, or any other characteristic protected under applicable federal civil rights law;
- Trade, profession, business activity, educational or industry membership, provided such activity is lawful under applicable federal and state law, including the lawful manufacture, distribution, sale, purchase, ownership, or use of firearms, the operation of fossil fuel, mining, or agricultural businesses, or participation in any other lawful industry;
- Health-related status or belief;

- Participation in, or refusal to participate in, any social justice, civil rights, affirmative action, ESG, DEI, or similar program or initiative, provided the individual or entity is in compliance with applicable law; or
- Any other lawful act, belief, or association.

Treasury should further require that the criteria, logic, and decision rules of any automated or algorithmic system used by a PPSI to make block, freeze, reject, or account termination decisions be fully disclosed to the PPSI's primary federal payment stablecoin regulator and made available to any affected customer upon request through a system in which the customer can take protective action through a reasonably accessible process, including the availability of human actors. A PPSI should not be permitted to operate a system whose decision criteria are unknown to the customers whose financial lives it affects and who may not be able to gather evidence admissible in court to support any claims of impropriety, illegality, or inaccessibility.

C. All Final Block, Freeze, Reject, Seize, and Burn Decisions Must Be Made by an Identified Human Officer, Not by Automated Execution

The Proposed Rule's silence on human review is among its most consequential omissions. Proposed § 1033.240 would require PPSIs to maintain the "technical capabilities, policies, and procedures" to block, freeze, and reject transactions — language that, as written, permits and may in practice encourage the full automation of these actions through smart contract execution without any human being in the decision loop at the moment an action is taken against a customer and thereafter. The GENIUS Act's mandate that PPSIs have such capabilities does not compel, and should not be read to authorize, the elimination of human judgment, and recourse, from the exercise of those capabilities.

Fully automated block, freeze, and rejection execution presents grave risks that a human-in-the-loop requirement would at least partially mitigate. First, automated systems make errors — false positives in sanctions screening and AML transaction monitoring are well-documented and common, and when a block, freeze, or rejection is executed by code rather than a compliance officer, the customer bears the burden of reversing an action that should never have been taken. Second, automated execution removes accountability: there is no identified human being who made the decision, who can be questioned about it, and who bears professional and legal responsibility for its accuracy and lawfulness. Third, automated systems are susceptible to discriminatory or viewpoint-based criteria that may be embedded in their logic and are difficult to detect or challenge precisely because no human reviewed the individual case, and as such, may be difficult or impossible to produce as evidence in any legal forum where proof of their existence is required. Fourth, the irreversible nature of certain stablecoin actions — particularly burning, which permanently destroys a customer's holdings — makes the case for mandatory human review especially compelling: a burned stablecoin cannot be restored if the automated decision was wrong. Finally, these decisions may have the power to destroy businesses, livelihoods, and even lives, and such decisions should be made by identifiable

humans who are legally accountable for their actions, or act as officers of their government or enterprise, and have the experience to understand not only the laws and regulations but the full context of the specific situation.

The appropriate model is not novel: it mirrors the existing compliance framework governing sanctions blocking actions and AML holds at traditional financial institutions, where automated monitoring systems flag potentially impermissible transactions for human review and a designated compliance officer makes the final determination. Automation serves a critical and legitimate function in that model — it allows PPSIs to surveil large transaction volumes efficiently, identify potential violations at scale, and bring flagged items to human attention promptly. What automation must not do is replace the compliance officer's judgment on whether the decision to block, freeze, reject, or burn is warranted in the specific case before the PPSI.

We therefore urge Treasury to amend proposed § 1033.240 to require that:

- While automated systems may under legally permissible conditions be used to surveil transactions, generate alerts, flag potentially impermissible activity, queue cases for review, and reach false positive determinations, the final decision to block, freeze, reject, seize, or burn any specific payment stablecoin transaction or customer holding must be made by an identified, named human compliance officer employed or contracted by the PPSI, who shall review the flagged transaction or holding, apply the PPSI's policies and applicable legal requirements to the specific facts, and personally authorize the action in writing before it is executed.
- The PPSI must maintain a written record of each block, freeze, rejection, seizure, or burn decision, identifying: (i) the compliance officer who authorized the action; (ii) the date and time of the authorization; (iii) the legal basis for the action; (iv) the specific facts reviewed by the officer in making the determination; and (v) whether the action was undertaken pursuant to a lawful order, an OFAC sanctions obligation, a SAR-related hold, or the PPSI's internal policies. Such records shall be retained for a period of no less than five years and made available to the PPSI's primary federal payment stablecoin regulator upon request.
- The foregoing human review requirement applies to all primary and secondary market blocks, freezes, rejections, seizures, and burns.
- No PPSI may structure its smart contracts, automated systems, or policies in a manner that delegates to code or other automation the authority to make final determinations to block, freeze, reject, or burn, whether that delegation is express or results from the practical absence of human review in the PPSI's compliance workflow. Treasury should confirm in examination guidance that a PPSI whose compliance workflow results in automatic execution of blocks, freezes, rejections, or burns without contemporaneous human review and authorization will be deemed to have a deficient AML/CFT program under proposed § 1033.210, regardless of whether any individual action resulted in an incorrect outcome.

We recognize that requiring human review of each flagged transaction imposes operational costs on PPSIs, particularly large-volume issuers. Treasury should seek comment on whether tiered safe harbors are appropriate — for example, permitting automated execution of OFAC SDN-list exact-match blocks while requiring human review for all other categories of action — but any such safe harbor must be narrowly drawn and must not permit the effective elimination of human review from the majority of decisions to block, freeze, and reject. The cost of false positives, wrongful freezes, blocks, rejections, and burns, and unaccountable automated enforcement against law-abiding customers is borne not by the PPSI but by the individuals whose access to their own funds has been the subject of interference. That asymmetry counsels strongly in favor of mandatory human review as the regulatory baseline.

II. THE "PUBLICLY AVAILABLE INFORMATION" CHARACTERIZATION OF BLOCKCHAIN TRANSACTION DATA CREATES SERIOUS FINANCIAL PRIVACY RISKS THAT THE PROPOSED RULE FAILS TO ADDRESS

The Proposed Rule, following the GENIUS Act, operates within a framework that treats transaction-level data recorded on public blockchains as "publicly available information." The implications of this characterization for financial privacy are profound and have not been adequately examined in the Proposed Rule.

Unlike bank records, which are protected from warrantless government access by the Right to Financial Privacy Act ("RFPA"), 12 U.S.C. §§ 3401 et seq., and from third-party commercial access by the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801 et seq., blockchain transaction records are permanently accessible to any actor with the computational capacity to analyze them. Chain analysis firms have demonstrated the ability to de-anonymize blockchain wallets at scale using commercially available tools, linking on-chain transactions to individual identities through a combination of PPSI KYC records and pattern analysis of on-chain behavior. Chain analysis firms may provide private information to government actors, or government actors may employ tools to obtain such private information themselves, which without legal process would otherwise be protected by the fourth Amendment. The practical effect is to create a permanent, searchable, and globally accessible record of every payment made by every PPSI customer — a surveillance architecture of a kind never before associated with a retail payments system.

While we recognize that the BSA's transaction monitoring and reporting framework requires PPSIs to collect and share certain transaction information with law enforcement, Treasury should take affirmative steps to limit the collateral use of blockchain transaction data for purposes unrelated to lawful AML/CFT and sanctions compliance. Specifically, we urge Treasury to:

- Amend the Proposed Rule to require PPSIs to implement, on a reasonable timeline, privacy-enhancing technologies that limit the public disclosure of transaction amounts, counterparty identities, and transaction metadata on public distributed ledgers, while preserving the ability

to make required disclosures to FinCEN, OFAC, and law enforcement through secure channels.

- Prohibit PPSIs from making transaction-level data available to commercial data brokers, advertising networks, or any third party that is not FinCEN, OFAC, a primary federal payment stablecoin regulator, a law enforcement agency acting pursuant to valid legal process, or the customer whose transaction data is at issue. Additionally provide for disclosure of any such violations to impacted customers and applicable regulators and levy penalties for any violations of such prohibition.
- Require PPSIs to notify customers promptly of any cybersecurity or information security incident affecting the customers' private keys, personally identifiable information, or financial data.
- Require a Privacy Impact Assessment as part of the PPSI application process, to be updated annually, addressing the risks to customer financial privacy associated with operation on a public distributed ledger and the measures the PPSI will implement to mitigate those risks.

III. THE PROPOSED RULE SHOULD ADDRESS THE INTERACTION BETWEEN BSA OBLIGATIONS AND THE RIGHT TO FINANCIAL PRIVACY ACT AND OTHER CONSUMER FINANCIAL PRIVACY PROTECTIONS

The BSA framework the Proposed Rule establishes for PPSIs will require PPSIs to collect substantial amounts of customer financial information, including for purposes of CDD, SAR filing, and CTR reporting, and PPSIs may collect additional transaction and other sensitive or private information for their own purposes. The Proposed Rule does not address the interaction between and among these BSA obligations, PPSI data collection and disclosure activities, and the financial privacy protections afforded by the RFPA, GLBA, and applicable consumer financial privacy regulations.

We urge Treasury to confirm in the preamble or guidance that:

- The BSA obligations imposed on PPSIs by the Proposed Rule do not preempt or displace the procedural protections of the RFPA with respect to government access to customer financial records held by PPSIs, except to the extent expressly required by the BSA and its implementing regulations.
- PPSIs that are subject to the GLBA and its implementing regulations remain subject to those obligations with respect to the collection, use, and sharing of customer financial information, and that the Proposed Rule does not authorize PPSIs to share customer financial data with third parties beyond what is required or permitted by the BSA, the RFPA, and the GLBA.
- PPSIs must include in their required customer disclosures a clear and plain-English explanation of the categories of customer financial information they collect, the purposes for which such information may be used, the persons or entities with whom such information may be shared, and any customer recourse for improper disclosure, consistent with applicable consumer financial protection requirements.

IV. CONCLUSION

Solari, Inc. respectfully urges FinCEN and OFAC to amend the Proposed Rule to address each of the concerns and recommendations set forth above. The regulatory framework that Treasury establishes for PPSIs at this foundational moment will shape the architecture of the U.S. payments system and the rights of Americans within it for decades to come.

The illicit finance risks that animate the Proposed Rule are real and serious, and Solari, Inc. supports robust, risk-based AML/CFT and sanctions compliance programs for PPSIs. But compliance frameworks that permit the wholesale automation of consequential enforcement actions — and that fail to affirmatively prohibit discriminatory or politically motivated use of block, seize, and freeze capabilities — will ultimately undermine both the rule of law and the integrity of the payments system they are meant to protect. Automated systems are tools; they must remain subject to human judgment, human accountability, and human law. Users should have confidence that these systems will protect their rights and privacy. A payments system that surveils, restricts, and controls the financial behavior of law-abiding Americans — however efficiently, and whether by human or algorithmic hand — is not a payments system that serves a free people.

We thank FinCEN and OFAC for the opportunity to submit these comments and respectfully request that the agencies carefully consider the concerns and recommendations set forth herein. We would welcome the opportunity to discuss these matters further with agency staff at their convenience.

Respectfully submitted,

/s/

Catherine Austin Fitts
President
Solari, Inc.

June 9, 2026