



October 19, 2026

U.S. Department of the Treasury
Attention: Office of General Counsel
1500 Pennsylvania Avenue NW
Washington, DC 20220

RE: GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale (August 18, 2026),
Docket No. TREAS–DO–2026–0496, RIN 1505–AC95

Dear Ladies and Gentlemen:

The Joint Center for Political and Economic Studies (“Joint Center”)¹ appreciates the opportunity to comment on the Department of the Treasury’s (“Treasury”) proposal (“Proposal”) implementing section 3 of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act).²

Stablecoins are increasingly promoted as financial tools that could expand access, reduce transaction costs, and create new economic opportunities. But those claims raise an important question for the Joint Center. If stablecoins are going to be presented as tools that could benefit Black communities, Treasury should examine whether those benefits are likely to reach Black households, businesses, and financial institutions in practice.

That question matters because the rules governing the emerging stablecoin market will help determine who can participate. Compliance requirements that are manageable for large financial institutions and digital asset firms may impose greater burdens on smaller institutions with fewer resources. Verification systems may also affect consumers differently depending on the information, documentation, and technology required to establish eligibility. The Joint Center therefore brings a distinct perspective to this rulemaking by focusing not simply on whether a stablecoin market can function, but on who can participate in that market and whether its potential benefits are broadly accessible.

The Joint Center’s comments focus on a discrete but consequential feature of the Proposal, namely the policies, procedures, and controls issuers and digital asset service providers may use to determine whether a person is located in the United States. Treasury squarely invites comment on this issue in Questions 38 and 62. Question 38 asks what policies, procedures, or controls should support a reasonable belief that an acquiring person is outside the United States. Question 62 asks what procedures should

¹ The Joint Center, known as America’s Black Think Tank, provides compelling and actionable policy solutions to eradicate persistent and evolving barriers to the full freedom of Black people in America. For more than fifty years, the Joint Center has served as a trusted forum for leading experts and scholars to engage in major public policy debates and advance ideas that strengthen Black communities. Through evidence-based research, analysis, convenings, and strategic communications, the Joint Center works to inform policymakers and support Black communities and a network of allies.

² U.S. Department of the Treasury, GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale, 91 Fed. Reg. 53,368 (Aug. 18, 2026), <https://www.govinfo.gov/content/pkg/FR-2026-08-18/pdf/2026-16796.pdf>.

support a reasonable belief that an offer or sale was not made to a person located in the United States. Together, those questions identify potential tools including customer identification and due diligence, account-opening information, geographic restrictions, device or network location checks, contractual representations, transaction monitoring, self-attestations, IP-address checks, identification documents, and other controls.³ Treasury also asks in Questions 81 through 87 about costs, information collection burdens, distributional effects, regulatory alternatives, compliance efficiency, and market participation.⁴

These questions have particular implications for Black consumers and the institutions that serve Black communities. As financial markets become increasingly digital, participation depends not only on whether a person or institution is legally eligible to participate, but also on whether the compliance systems governing access can reliably recognize and verify them. Requirements that appear neutral on their face can have different practical consequences depending on the cost of compliance, the information required to establish eligibility, and the ability of consumers and institutions to correct erroneous determinations. These questions are especially important as policymakers consider whether emerging financial technologies will expand access to the financial system or reproduce existing barriers in a new form.

Section 3 requires effective mechanisms for distinguishing activity that occurs in the United States from activity outside the United States. But the design of those mechanisms can also determine who can practically participate in the market. A person or institution may satisfy the substantive requirements of the law but still be excluded if the compliance infrastructure cannot reliably recognize or verify the facts that establish eligibility.

The Joint Center does not recommend weaker compliance standards. We recommend standards that are strong, risk-based, technology-neutral, and workable across institutions with different business models and resources. Treasury can preserve the proposed reasonable belief framework while reducing unnecessary duplication, avoiding overreliance on any single technical signal, creating clear pathways for reliance on appropriately regulated intermediaries, and ensuring that legitimate users have a way to resolve erroneous determinations. Treasury should also more fully evaluate how the fixed costs and error rates associated with verification could affect Black consumers, institutions serving Black communities, smaller market participants, and other populations that may experience barriers to participation.

Location Verification Is Central to Whether the Proposed Framework Is Workable

The proposed rule makes location an important part of determining whether activity falls within section 3. In proposed §§ 1523.2(c) and 1523.3(e), Treasury describes circumstances in which an issuer or digital asset service provider would be deemed not to have engaged in covered U.S. activity when it reasonably believes the acquiring person is outside the United States and satisfies other conditions, including maintaining reasonably designed policies, procedures, and controls.⁵

For the Joint Center, the concern is not that location verification is inherently harmful to Black consumers, but that poorly designed requirements could reinforce existing barriers to financial participation. Black households are more likely than white households to be unbanked or underbanked, while smaller institutions serving Black communities may have fewer resources to absorb new compliance costs. Verification approaches that depend heavily on existing financial relationships, particular forms of documentation, or costly technology therefore deserve careful scrutiny. Treasury should evaluate whether these requirements increase failure rates, add burdens, or reduce participation for consumers and institutions that already face barriers to the financial system. Treasury should give firms

³ GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale, 91 Fed. Reg. at 53,378 (Question 38), 53,384 (Question 62).

⁴ Id. at 53,388–89 (Questions 81–87, requesting comment on costs, benefits, distributional effects, alternatives, compliance efficiency, market participation, and information collection burdens).

⁵ Id. at 53,377–78 (proposed § 1523.2(c)), 53,384 (proposed § 1523.3(e)).

clear obligations, but it should avoid turning a location determination into a rigid test that assumes one form of information will work equally well for every person, institution, or business model.

Treasury identifies several possible tools for determining location, including customer information, identification documents, IP addresses, device information, transaction monitoring, and other forms of verification. Those tools can provide useful information, but no single method will be accurate in every circumstance. Technical guidance on IP-based geolocation recognizes that errors and inaccuracies can occur and recommends verification when data conflict.⁶

Treasury's proposed reasonable belief standard is therefore the right starting point. The final rule should preserve a flexible approach that allows firms to consider the facts and circumstances rather than converting the list of possible controls in Questions 38 and 62 into a mandatory checklist.

Treasury Should Preserve a Flexible, Risk-Based Approach

Different institutions will have different information available to them. A large retail platform may have extensive customer and device data, while a smaller institution or an issuer that distributes through regulated intermediaries may have a different set of reliable information. Treasury should allow firms to use a reasonable combination of information that fits their business model, customers, and risk profile.

A flexible approach would also make the rule more durable as technology changes. Treasury should establish the outcome firms must achieve and the basic safeguards expected, while allowing the specific tools used to verify location to evolve over time.

Treasury should also make clear that no single technical signal automatically controls when other reliable information points in a different direction. An IP address, device signal, or self-attestation may be relevant, but each should be considered as part of the overall determination. This approach would help deter evasion while reducing the risk that legitimate users are excluded because one data point is incomplete or wrong.

By analogy, federal digital identity guidance offers a useful general design principle. NIST recommends giving applicants multiple proofing options and providing exception handling to promote access for people with different means, capabilities, and technologies.⁷

Verification Costs Could Affect Smaller Institutions and Market Participation

Treasury's Regulatory Flexibility Act discussion states its preliminary view that the Proposal would not have a significant economic impact on a substantial number of small entities, while also requesting comment on that issue.⁸ The final analysis should look more closely at the costs associated with location verification, including the cost of technology, outside vendors, legal and compliance staff, ongoing monitoring, and review of difficult cases.

Evidence from banking regulation shows why scale matters. A 2025 CSBS working paper found that smaller community banks reported higher regulatory compliance cost burdens than larger institutions across several categories of expense.⁹ The study does not measure stablecoin regulation, but it illustrates a broader point that fixed compliance costs can fall more heavily on smaller institutions.

⁶ Erik Kline et al., A Format for Self-Published IP Geolocation Feeds, RFC 8805 § 3.3 (Aug. 2020), <https://www.rfc-editor.org/rfc/rfc8805.html>.

⁷ National Institute of Standards and Technology, *Digital Identity Guidelines: Identity Proofing and Enrollment*, NIST SP 800-63A-4, "Identity Proofing Overview" (July 2025), <https://pages.nist.gov/800-63-4/sp800-63a/proofing/>.

⁸ GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale, 91 Fed. Reg. at 53,387–88.

⁹ Thomas F. Siems, Do Banking Regulations Disproportionately Impact Smaller Community Banks?, CSBS Working Paper 25-01 (July 29, 2025), https://www.communitybanking.org/-/media/files/communitybanking/2025-papers/national-survey_siems.pdf.

That concern matters to the Joint Center because smaller institutions, including minority depository institutions, community development financial institutions, and community banks, often play an important role in communities that have historically had less access to mainstream financial services. A rule that is relatively easy for a large firm with extensive technology and compliance resources to absorb may present a more significant barrier for a smaller institution considering whether and how to participate in the stablecoin market.

Treasury should therefore examine location verification costs by business model and, where data permit, by firm size. It should also consider the cumulative burden of overlapping GENIUS Act requirements and look for opportunities to coordinate with FinCEN, OFAC, and the primary federal payment stablecoin regulators. Treasury itself asks how the costs and benefits of this Proposal should be analyzed alongside related regulatory frameworks, and other stakeholders have similarly urged consistency across GENIUS Act compliance regimes.¹⁰

Treasury Should Avoid Duplicating Verification Already Performed by Regulated Intermediaries

Question 38 asks how responsibility should be divided when an issuer distributes stablecoins through a digital asset service provider or another intermediary. The Joint Center believes Treasury should preserve accountability without requiring every entity in the chain to repeat the same verification work.

A related 2026 GENIUS Act proposal provides a useful model. The proposed Customer Identification Program rule would allow a permitted payment stablecoin issuer, subject to specified conditions, to rely on another regulated financial institution to perform portions of the issuer's customer identification program.¹¹ Location verification under section 3 is a different legal question, but the same basic principle is useful here.

Where a regulated intermediary already performs reliable location verification, an issuer should be able to rely on that work when appropriate. Treasury can condition such reliance on clear agreements, reasonable oversight, access to necessary information, and procedures for addressing problems or red flags.

This would be particularly helpful for smaller institutions that may need to partner for specialized compliance capabilities rather than build every function internally. Reliance should not become a way to avoid responsibility. It should be a way to prevent unnecessary duplication when another regulated entity is already performing the relevant work.

Coordination across federal regulators is also important. Where legally permissible, firms should be able to reuse information that has already been reliably verified rather than repeatedly collecting the same information for overlapping regulatory requirements. At the same time, Treasury should protect data security and privacy and recognize that identity, sanctions, anti-money laundering, and location rules serve different statutory purposes.

Consumers Need a Practical Way to Correct Verification Errors

Any verification system can get a legitimate determination wrong. A person may have information that is incomplete, outdated, or inconsistent across records, and automated systems may not always capture the circumstances that matter under Treasury's rule. The relevant question is not whether errors can be eliminated entirely, but whether firms have a reasonable way to identify and correct them.

¹⁰ GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale, 91 Fed. Reg. at 53,388–89 (Question 84); American Bankers Association, Letter to the FDIC on Permitted Payment Stablecoin Issuers (Aug. 6, 2026), <https://www.aba.com/advocacy/policy-analysis/letter-to-the-fdic-on-ppsi>.

¹¹ Financial Crimes Enforcement Network et al., Permitted Payment Stablecoin Issuer Customer Identification Program, 91 Fed. Reg. 37,234, 37,269–70 (proposed June 22, 2026) (proposed 31 C.F.R. § 1033.220(a)(6)), <https://www.federalregister.gov/documents/2026/06/22/2026-12460/permitted-payment-stablecoin-issuer-customer-identification-program>.

Treasury should therefore expect firms relying on the proposed safe harbors to maintain a practical process for resolving conflicting information. Legitimate users should have a way to provide clarifying information and obtain review when a location determination appears to be wrong. Where appropriate, firms should be able to escalate difficult cases to trained personnel rather than relying exclusively on an automated decision.

By analogy, federal digital identity guidance recognizes the importance of redress when identity proofing fails, is delayed, or creates difficulties.¹² Treasury need not import that framework into section 3, but the underlying principle is relevant. A compliance system should be judged not only by how often it blocks a transaction, but also by whether it can distinguish between an attempted evasion and a legitimate user who needs an error corrected.

Treasury should encourage firms to track basic outcomes such as failed or indeterminate checks, reversals after review, resolution times, and customer abandonment. Those measures would help Treasury and regulated firms understand whether particular approaches are working in practice and whether they impose unnecessary burdens on legitimate users.

Treasury Should Examine Effects on Black Consumers and Institutions Serving Black Communities

Treasury expressly asks about the Proposal's costs, benefits, distributional effects, information collection burdens, compliance efficiency, and effects on market participation.¹³ For the Joint Center, that inquiry should include who bears the costs of verification, who is more likely to encounter difficulty completing it, and whether the compliance framework creates barriers for smaller institutions that may want to participate.

These questions are relevant to Black communities because consumers and institutions enter new financial markets from different starting points. The FDIC's 2023 national survey found that 10.6 percent of Black households were unbanked, compared with 1.9 percent of white households, and that 23.8 percent of Black households were underbanked, compared with 10.1 percent of white households.¹⁴ The same survey also shows substantial use of mobile banking among Black households. Together, these data underscore why digital availability should not be assumed to produce equal practical access.

Some location verification methods may be inexpensive and easy for most users. Others may depend on established account relationships, particular forms of identification, persistent device information, or third-party data. Treasury should examine how these methods perform in practice, including whether legitimate users are more likely to fail verification, abandon a transaction, or require manual review.

Treasury has recognized similar concerns in other contexts. Its 2024 National Strategy for Financial Inclusion states that customer identification and verification requirements should be risk-based and should not unnecessarily limit access to financial services for underserved communities.¹⁵ Treasury's 2023 De-Risking Strategy likewise found that the cost of AML/CFT compliance, available resources, lack of clarity regarding regulatory expectations, and other regulatory burdens can contribute to de-

¹² National Institute of Standards and Technology, Digital Identity Guidelines: Identity Proofing and Enrollment, NIST SP 800-63A-4, Redress Requirements (July 2025), <https://pages.nist.gov/800-63-4/sp800-63a/ial-general/#redress-requirements>.

¹³ See *supra* note 4.

¹⁴ Federal Deposit Insurance Corporation, 2023 FDIC National Survey of Unbanked and Underbanked Households: Executive Summary 6, fig. ES.6 (2024), <https://www.fdic.gov/household-survey/2023-fdic-national-survey-unbanked-and-underbanked-households-executive-summary>.

¹⁵ U.S. Department of the Treasury, *National Strategy for Financial Inclusion in the United States: Fostering Financial Access, Resilience, and Well-Being for All* 20–21 (2024), <https://home.treasury.gov/system/files/136/NSFI.pdf>

risking decisions.¹⁶ Those initiatives address different legal regimes, but they reflect an important principle for this rulemaking. Compliance requirements can shape access as well as safety.

The Joint Center does not recommend that Treasury require issuers or digital asset service providers to collect race or ethnicity solely for section 3 compliance. That could create additional privacy and security concerns. Treasury can instead use existing data, targeted research, complaints, supervisory reviews, surveys, and other privacy protective methods to evaluate whether verification systems create different outcomes across populations.

Treasury should also consider how the rule may affect the institutions that serve Black communities. If compliance costs are largely fixed, a requirement that is manageable for a large firm may discourage a smaller institution from entering the market or may force it to rely heavily on a small number of third-party vendors. Treasury should assess whether its approach unnecessarily raises entry costs or limits the range of institutions able to participate.

This is where the Joint Center's broader concern about stablecoin access becomes concrete. If stablecoins are promoted as a way to expand financial access or create new economic opportunities, Treasury should examine whether the regulatory framework gives Black consumers, Black-owned businesses, minority depository institutions, community development financial institutions, and other smaller institutions a realistic path to participate. That does not require weaker standards. It requires asking whether strong standards are designed in a way that can be met by more than the largest market participants.

Recommendations

The Joint Center recommends that Treasury

1. Preserve a flexible, risk-based approach to location verification rather than requiring every firm to use the same set of verification tools.
2. Examine how verification requirements affect Black consumers and institutions serving Black communities, including whether certain approaches create unnecessary barriers to participation or impose greater costs on smaller institutions.
3. Avoid unnecessary duplication by allowing firms to rely on verification already performed by other regulated entities when appropriate and by coordinating overlapping federal requirements.
4. Require practical ways to correct verification errors so legitimate consumers are not excluded because of incomplete or inaccurate information.
5. Evaluate the real-world effects of the final rule, including failed verifications, consumers giving up during the process, compliance costs, and whether smaller institutions have a realistic path to participate.

Conclusion

The Joint Center supports strong and effective rules for the emerging stablecoin market. But as the Treasury develops those rules, it should also consider who can participate and who may be left out.

Stablecoins are increasingly promoted as tools that could expand financial access, lower costs, and create new economic opportunities. If those benefits are expected to extend to Black communities, the rules governing the market should not create unnecessary barriers for Black consumers, Black-owned businesses, minority depository institutions, community development financial institutions, or other institutions that serve Black communities.

¹⁶ U.S. Department of the Treasury, The Department of the Treasury's De-Risking Strategy 2 (Apr. 2023), https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf.

That does not require weaker standards. It requires Treasury to consider how its rules will work in practice, including whether compliance costs fall more heavily on smaller institutions, whether legitimate consumers can be wrongly excluded, and whether those errors can be corrected.

For the Joint Center, the central question is not simply whether the stablecoin market can function. It is whether Black households, businesses, and institutions will have a meaningful opportunity to participate in and benefit from that market. Treasury should keep that question in view as it finalizes the rule.

The Joint Center appreciates the opportunity to comment on this important rulemaking and would welcome continued engagement as Treasury develops the final rule.

For questions regarding these comments, please contact Cantrell Dumas, Senior Researcher, Financial Regulation and Policy, Joint Center for Political and Economic Studies, 633 Pennsylvania Ave., NW, Washington, DC 20004, at cantrell.dumas@jointcenter.org.