June 9, 2026

The Honorable Andrea M. Gacki
Director
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Mr. Bradley T. Smith
Director
Office of Foreign Assets Control
U.S. Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Re: Response to Notice of Proposed Rulemaking Regarding Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements

Dear Director Gacki and Director Smith,

On behalf of the American Fintech Council (AFC),[1] the largest and most diverse trade association representing financial technology companies and innovative banks, I submit this comment letter in response to the joint proposed rulemaking (Proposed Rulemaking) issued by the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) concerning Anti Money Laundering and Countering the Financing of Terrorism (AML/CFT) and sanctions compliance obligations applicable to permitted payment stablecoin issuers (PPSIs) under the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act).[2]

On behalf of more than 150 member companies and partners, AFC supports regulatory frameworks that promote responsible innovation, safeguard the integrity of the financial system, and maintain strong protections against illicit finance while preserving operational feasibility and continued technological advancement. AFC's membership includes innovative banks, payments companies, financial technology firms, digital asset participants, and infrastructure providers that

[1] American Fintech Council's (AFC) membership spans banks, non-bank lenders, payments providers, EWA providers, loan servicers, credit bureaus, and personal financial management companies.

[2] Financial Crimes Enforcement Network and Office of Foreign Assets Control, "Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements," *Federal Register* 91, no. 69 (April 10, 2026): 18582–18642, https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism.

operate across a wide range of financial services activities, including payments, compliance technology, transaction monitoring, digital asset infrastructure, and bank-fintech partnerships.

AFC appreciates Treasury's recognition that payment stablecoin issuers should be subject to meaningful AML/CFT and sanctions obligations consistent with the risks associated with digital asset activity. The proposed rule appropriately reflects the importance of preventing illicit finance activity within the payment stablecoin ecosystem while also acknowledging the need for requirements that are tailored to the size, complexity, and technological architecture of the entities involved. As Treasury finalizes this framework, however, it is essential that implementation remain appropriately risk based, operationally practicable, technologically neutral, and aligned with existing Bank Secrecy Act frameworks. Regulatory expectations that are overly rigid, process oriented, or disconnected from the operational realities of blockchain based systems may inadvertently undermine innovation, discourage responsible market participation, and reduce the effectiveness of AML/CFT compliance efforts. AFC therefore respectfully offers the following recommendations regarding the proposed rulemaking.

I. AFC Supports a Tailored AML/CFT and Sanctions Framework for Payment Stablecoin Issuers that Preserves Operational Feasibility and Promotes Responsible Innovation

As Treasury implements AML/CFT and sanctions obligations for PPSIs, the resulting framework should appropriately account for the operational realities, technological architecture, and transactional structure of blockchain based payment systems. Although payment stablecoins may implicate illicit finance risks that warrant meaningful oversight, the compliance framework should remain appropriately tailored to the functions actually performed by issuers and the degree of operational visibility and control they possess within the broader ecosystem.

Payment stablecoin issuers operate within a fundamentally different transactional environment than many traditional financial institutions. Blockchain based systems often involve multiple intermediaries, decentralized transaction flows, automated smart contract execution, and secondary market activity occurring outside the direct involvement of the issuer itself. As a result, compliance expectations should remain grounded in what issuers can reasonably monitor, control, and supervise in practice rather than imposing obligations that are disconnected from the operational structure of blockchain based payment systems.

A risk-based framework is particularly important in the context of transaction monitoring, sanctions compliance, and testing obligations. Not all risks present equivalent exposure or require identical levels of review, escalation, or testing frequency. Certain transaction channels, customer segments, geographies, or operational functions may present heightened exposure to illicit finance risk and therefore warrant enhanced scrutiny, while lower risk activities may reasonably be subject to more streamlined controls. A framework that treats all categories of risk identically may divert institutional resources away from the areas of greatest supervisory and national security concern.

Treasury should therefore make clear that testing, monitoring, and broader compliance expectations may be calibrated according to the relative risk profile associated with particular

activities, products, customer segments, and transaction flows. Allowing institutions to tailor the intensity and frequency of compliance measures in this manner would better align supervisory expectations with actual risk exposure while enabling compliance resources to remain focused on areas of heightened illicit finance concern.

The proposed framework should also avoid creating unnecessary operational burdens where existing controls, systems, or supervisory structures already achieve the intended compliance objective. Requiring entirely new infrastructure, duplicative reporting systems, or bespoke compliance processes disconnected from existing Bank Secrecy Act frameworks may increase cost and complexity without producing corresponding improvements in AML/CFT effectiveness. Treasury should instead encourage integration with existing compliance systems and allow institutions to leverage current transaction monitoring tools, suspicious activity reporting processes, sanctions screening infrastructure, and governance frameworks wherever practicable.

This principle is particularly important given the rapid evolution of financial technology and digital asset infrastructure. Novel technologies frequently enhance AML/CFT compliance capabilities by improving transaction visibility, automating risk detection, increasing monitoring precision, and reducing manual error rates. Advanced analytics, blockchain monitoring tools, machine learning systems, and automated screening technologies increasingly allow institutions to identify suspicious patterns and sanctions risks more effectively than traditional manual review processes. Treasury should therefore ensure that the final rule supports continued innovation and supervisory acceptance of responsible regulatory technology solutions rather than inadvertently discouraging their deployment through overly prescriptive requirements.

II. AFC Supports Clear Distinctions Between Primary Market Activity and Secondary Market Activity to Promote Effective and Operationally Practicable Compliance Expectations

Treasury is appropriately recognizing the importance of distinguishing between primary market activity and secondary market activity within the payment stablecoin ecosystem, and the final framework should continue to refine and operationalize that distinction with precision. Maintaining clear regulatory distinctions between these categories is essential to ensuring that compliance obligations remain operationally practicable and appropriately tailored to the actual degree of control exercised by a PPSI.

PPSIs generally maintain the greatest degree of visibility and direct customer interaction in connection with issuance, redemption, custody, and other primary market functions. By contrast, many forms of secondary market activity occur without direct issuer involvement beyond the operation of the relevant smart contract infrastructure. Imposing identical compliance expectations across both categories of activity could create operational obligations that exceed the practical capabilities of issuers, particularly where issuers lack direct access to customer relationships or transactional visibility. Treasury should therefore further clarify that AML/CFT and sanctions obligations applicable to PPSIs should be calibrated to the level of operational control, customer interaction, transactional visibility, and practical risk mitigation capability associated with the relevant activity. This distinction is particularly important in decentralized or

intermediary driven transaction environments where secondary market transfers may occur independently of any direct involvement by the issuer.

While the distinction between primary market and secondary market activity remains an important component of a risk-based compliance framework, it should not be interpreted as a complete boundary on issuer responsibility. In certain circumstances, compliance responsibilities should reflect not only what an issuer directly controls, but also what it can reasonably influence through the design and operation of its program. Treasury should therefore ensure that compliance expectations appropriately reflect risks that issuers can reasonably identify, influence, or mitigate while avoiding obligations tied to activity that falls beyond their practical visibility or operational control. Consistent with this approach, issuer responsibility should be evaluated not solely by reference to whether a transaction occurs within the primary or secondary market, but also by the extent to which an issuer can reasonably influence risk outcomes through the design of its compliance program, operational controls, and relationships with relevant ecosystem participants.

Similarly, Treasury should ensure that compliance obligations remain platform agnostic and avoid unintentionally disadvantaging particular blockchain architectures, operational models, or technological designs. The objective of the framework should be effective risk mitigation and sanctions compliance rather than mandating any singular technological approach. A principles based framework focused on measurable compliance outcomes will better accommodate continued technological evolution while maintaining strong safeguards against illicit finance risk.

Treasury should also provide additional clarity regarding the role of third-party service providers and ecosystem participants operating within the payment stablecoin environment. Exchanges, custodians, compliance vendors, analytics providers, infrastructure firms, and other intermediaries frequently play important roles in transaction monitoring, customer due diligence, sanctions screening, and fraud prevention. Clear guidance regarding the allocation of responsibilities among ecosystem participants would improve operational coordination and reduce uncertainty regarding supervisory expectations.

III. AFC Supports Platform Agnostic and Risk Based Compliance Standards that Encourage Continued Innovation in AML/CFT Capabilities

Novel technologies increasingly play a critical role in strengthening AML/CFT and sanctions compliance capabilities throughout the financial services sector. Blockchain analytics, automated transaction monitoring tools, artificial intelligence driven risk detection systems, and advanced sanctions screening technologies often enhance institutional visibility into suspicious activity and improve the precision and efficiency of compliance functions. Treasury should therefore ensure that the final rule encourages continued adoption of responsible compliance technologies rather than inadvertently discouraging innovation through overly rigid or prescriptive requirements.

A principles-based framework focused on effective risk mitigation and measurable compliance outcomes will better accommodate continued technological development while preserving strong safeguards against illicit finance activity. Institutions should retain flexibility to deploy

compliance solutions that are appropriately calibrated to their business models, transaction structures, and operational risk profiles rather than being required to adopt uniform technological processes or procedures.

Importantly, flexibility in implementation should not be interpreted as a reduction in compliance expectations where payment stablecoin activity presents risks comparable to other regulated payment activities. Treasury should continue to focus on the effectiveness of compliance outcomes rather than prescribing particular technological methods for achieving them. Payment stablecoin issuers should retain discretion to leverage blockchain analytics, automated screening tools, transaction monitoring systems, wallet screening capabilities, and other risk based controls that are appropriately calibrated to their business models and risk profiles, provided that such measures effectively address applicable AML/CFT and sanctions risks.

Consistent with this principles-based approach, supervisory expectations should remain sufficiently flexible to accommodate the rapid pace of technological development within the digital asset ecosystem. Prescriptive compliance mandates tied to particular systems, operational models, or technological configurations may quickly become outdated as blockchain infrastructure and compliance capabilities continue to evolve. A more adaptable framework centered on measurable compliance effectiveness and sound risk management principles would better support long term innovation while preserving strong safeguards against illicit finance activity.

Regulatory clarity is also particularly important for innovative banks and bank-fintech partnerships participating in the payment stablecoin ecosystem. These arrangements frequently involve multiple entities operating under distinct supervisory frameworks while collectively contributing to compliance, operational resilience, and financial innovation. Treasury should therefore continue refining guidance regarding the allocation of compliance responsibilities among banks, technology providers, stablecoin issuers, custodians, and other service providers to reduce operational uncertainty and support effective coordination across the ecosystem.

Treasury should also continue to promote transparency regarding supervisory expectations, typologies, and emerging illicit finance risks. Greater information sharing between regulators and industry participants would strengthen institutional understanding of evolving threats and improve the effectiveness of AML/CFT programs across the financial services ecosystem. Public guidance, typology reports, and coordinated supervisory feedback mechanisms can significantly enhance compliance outcomes while reducing uncertainty and unnecessary operational friction.

* * *

AFC appreciates the opportunity to provide comments regarding this important proposed rulemaking. AFC supports appropriately tailored AML/CFT and sanctions obligations for payment stablecoin issuers that strengthen protections against illicit finance while preserving innovation, operational feasibility, and continued development within the digital asset ecosystem.

A properly calibrated framework should remain risk based, platform agnostic, and outcomes oriented while recognizing the operational realities associated with blockchain based financial

activity. Such an approach will better position regulated payment stablecoin issuers to maintain effective compliance programs, support responsible innovation, and contribute to the continued competitiveness and integrity of the United States financial system.

We appreciate Treasury's consideration of these comments and welcome continued engagement on these issues.

Sincerely,

Ian P. Moloney
Chief Policy Officer
American Fintech Council