anchorage digital bank

June 9, 2026
VIA REGULATIONS.GOV
Docket No. FINCEN-2026-0100

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

Office of Foreign Assets Control
U.S. Department of the Treasury
Washington, DC 20220

RE: 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)

To Whom It May Concern:

Anchorage Digital Bank, National Association ("ADB") appreciates the opportunity to comment on the joint notice of proposed rulemaking ("NPRM")[1] issued by the Financial Crimes Enforcement Network ("FinCEN") and the Office of Foreign Assets Control ("OFAC") implementing the anti-money laundering, countering the financing of terrorism ("AML/CFT"), and sanctions compliance provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (the "GENIUS Act") for permitted payment stablecoin issuers ("PPSIs").[2]

ADB has operated as a federally chartered bank regulated by the United States Office of the Comptroller of the Currency (the "OCC") for over five years. During this time, it has become the industry leader in digital asset custody, designed for security and asset accessibility, with tens of billions of digital assets under custody for institutional clients. In 2025, ADB also became the first federally chartered stablecoin issuer, and it expects to become a PPSI pursuant to the GENIUS Act once the implementing framework is effective. ADB currently issues five stablecoins (USAT, USDGO, USDPT, fUSD, and USDtb) and expects to begin issuing others in the near future, in each case for ADB's customer base and using smart contracts that provide ADB with issuer-level administrative controls.

ADB commends FinCEN and OFAC for the considered, risk-based approach reflected in the NPRM and for harmonizing the proposed obligations with the existing Bank Secrecy Act ("BSA") framework wherever possible. As the NPRM recognizes, the division of the payment stablecoin ecosystem into "primary market" and "secondary market" activity, and the different ways in which the AML and sanctions regimes treat that division, is the defining architectural feature of the

[1] Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, 91 Fed. Reg. 18,582 (Apr. 10, 2026) (the "NPRM").

[2] Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, 139 Stat. 419 (2025) (codified at 12 U.S.C. §§ 5901-5916).

proposal.[3] ADB writes for three principal reasons. First, ADB supports FinCEN's decision to scope AML monitoring and suspicious activity reporting to the primary market, and it seeks clarification that the proposal's secondary market sanctions obligations be applied on a reasonable, risk-based basis. Second, ADB responds to FinCEN's express request for comment on whether any proposed obligation would make compliance by an entity that is both a bank and a PPSI legally or practically impossible. Third, ADB offers targeted clarifications on the AML/CFT program, enhanced due diligence, and sanctions compliance program provisions. We address each in turn below.

I. Summary of ADB and Its Payment Stablecoin Activities

ADB issues each of its stablecoins one-to-one against GENIUS Act-ready reserves and serves a predominantly institutional customer base, including digital asset exchanges that intermediate access to ADB-issued stablecoins. ADB does not interact directly with the large population of downstream retail holders who transact in ADB-issued stablecoins on the secondary market. Like most stablecoin issuers, ADB uses smart contracts to issue, redeem, and (where required by law or a lawful order) freeze, block, or burn its stablecoins. ADB therefore maintains, and intends to continue to maintain, the issuer-level technical capabilities contemplated by proposed 31 C.F.R. § 1033.240.

Because ADB is an uninsured national bank, it would be subject to the BSA both as a bank under 31 C.F.R. Part 1020 and as a PPSI under proposed Part 1033, and to OFAC's proposed sanctions compliance program requirements under proposed 31 C.F.R. Part 502. ADB's comments are informed by its experience operating an enterprise-wide BSA/AML and sanctions compliance program as a federally chartered institution and as the first federally chartered issuer of a stablecoin.

II. The Asymmetry Between the AML and Sanctions Regimes Is the Central Design Choice of the Proposal, and the Secondary Market Sanctions Obligation Should Be Clarified to Be Risk-Based and Reasonable

The NPRM's defining feature is that the AML/CFT program, customer due diligence, and suspicious activity reporting obligations stop at the primary market, while the sanctions-related block, freeze, and reject obligations, together with OFAC's sanctions compliance program requirement, extend to the full lifecycle of a stablecoin, including all secondary market activity.[4] ADB supports the AML scoping decision and the flexible, technology-neutral approach to the block/freeze/reject capability. ADB respectfully asks the agencies to clarify, however, that the secondary market sanctions obligation does not impose a freestanding duty on a PPSI independently to identify every blocked person transacting in its stablecoin on the secondary market. Taken literally and combined with strict liability, such a duty would be practically impossible to satisfy.

[3] NPRM, 91 Fed. Reg. at 18,585 (describing "primary market" and "secondary market" activity).

[4] *Compare* NPRM, 91 Fed. Reg. at 18,592 (no AML secondary market monitoring requirement), 18,604 (FinCEN "is not contemplating application of CDD to secondary market activity"), and 18,607 (no secondary market SAR obligation), with *id*. at 18,605, 18,616, and 18,619 (sanctions block, freeze, and reject and effective sanctions program obligations extending to secondary market activity and the full lifecycle of a payment stablecoin).

a. ADB supports FinCEN's decision not to impose AML monitoring or SAR obligations on secondary market activity.

FinCEN has preliminarily determined not to require PPSIs, as part of an AML/CFT program, to monitor secondary market activity or to file suspicious activity reports ("SARs") on secondary market transfers, and proposes § 1033.320(g) to confirm that a secondary market transfer is not a "transaction" conducted by, at, or through a PPSI merely because it results in an interaction with the PPSI's smart contract.[5] ADB strongly supports this determination. As FinCEN recognizes, a PPSI often cannot identify the actor behind a secondary market transfer and may have only limited, smart contract-level visibility into such transfers. A blanket secondary market monitoring or reporting mandate would compel global surveillance of transfers, generate "defensive" SARs, and impose substantial burden disproportionate to the marginal information it would yield, particularly where other BSA-regulated institutions are better positioned to observe and report the activity. ADB agrees that the burden of such a requirement would outweigh its benefits, and we encourage FinCEN to retain this approach in the final rule.[6]

b. ADB supports the flexible, non-prescriptive approach to the block, freeze, and reject capability.

Proposed § 1033.240(a) requires a PPSI to maintain "technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions" that violate federal or state law, including with respect to secondary market activity.[7] ADB supports FinCEN's decision not to prescribe how a PPSI must implement this capability, which appropriately accommodates differences in stablecoin architecture and anticipates future technological change. ADB maintains issuer-level controls of this kind today and is well positioned to comply. ADB also supports FinCEN's clarification that this provision does not require a PPSI to make an independent determination that a transaction violates the law. Rather, the use of those capabilities is dictated by other legal authorities, such as OFAC sanctions, court orders, and lawful orders.[8]

c. The agencies should clarify that a PPSI is not strictly liable for failing independently to identify blocked persons transacting on the secondary market through its smart contract.

ADB's principal concern arises from the interaction of three features of the proposal. First, the preamble explains that a PPSI's capabilities, policies, and procedures should account for "identifying and blocking or rejecting" transactions that violate sanctions, and that a PPSI must have the capability "to identify and block stablecoins traded by blocked persons on the secondary market when PPSIs exercise possession or control of such stablecoins, including through smart contracts."[9] Second, OFAC's proposed definition of "payment stablecoin-related activity" reaches all

---

[5] *Id*. at 18,592, 18,607; proposed 31 C.F.R. § 1033.320(g).

[6] *Id*. at 18,607 (FinCEN "seeks comment on its preliminary determination that PPSIs should not be obligated to provide SAR reporting on the secondary market").

[7] *Id.* at 18,604-05; proposed 31 C.F.R. § 1033.240(a); *see* GENIUS Act § 4(a)(5)(A)(iv), 12 U.S.C. § 5903(a)(5)(A)(iv).

[8] *Id*. at 18,605 (the provision "would not require a PPSI to make an independent determination that a transaction violates federal or state law"; rather, "the use of technological capabilities will be dictated by other federal or state laws, rules, or regulations, as well as court orders").

[9] *Id.* at 18,605 (a PPSI's capabilities, policies, and procedures "should account for identifying and blocking or rejecting payment stablecoin-related transactions that would violate U.S. sanctions," and further providing that

activity involving the stablecoin "from the time of issuance until the payment stablecoin's removal from circulation, whether on the primary or secondary market,"[10] and OFAC's proposed internal controls element requires internal controls "applicable to all payment stablecoin-related activity, whether on the primary or secondary market, that identifies, blocks, and/or rejects" transactions that would violate U.S. sanctions across that full lifecycle.[11] Third, OFAC enforces its sanctions on a strict liability basis, such that a U.S. person may be held liable "even if such person did not know or have reason to know that it was engaging in a prohibited transaction."[12]

The capability to act once a sanctioned actor or address has been identified, whether by freezing, blocking, burning, or rejecting, is technologically achievable and is something ADB supports. The difficulty lies in the duty to identify the sanctioned actor in the first instance. On the secondary market, a PPSI interacts with the transfer only through its smart contract. It frequently cannot determine who controls a counterparty wallet or whether that party is a blocked person. Requiring a PPSI independently to identify blocked persons transacting in its stablecoin among the entire universe of secondary market activity, with strict liability, is in tension with FinCEN's conclusion that PPSIs should not be required to monitor that same secondary market activity for BSA/AML purposes.

ADB respectfully requests that the agencies clarify the final rule and its preamble in three related respects. ADB asks the agencies to confirm that the obligations under § 1033.240(a) and § 502.201(b)(3) require a PPSI to maintain the technical capability to interdict secondary-market transactions and to act on identifications supplied by operative legal authority, such as OFAC's designation of specific digital-currency addresses on the Specially Designated Nationals ("SDN") List, lawful orders, and court orders, together with risk-based screening reasonably designed to detect those identifiers, and that these obligations do not impose a freestanding duty to surveil and adjudicate the sanctions status of every secondary market counterparty address.

ADB further asks the agencies to confirm that, consistent with the risk-based standard OFAC itself articulates for internal controls, a PPSI that designs, implements, tests, and maintains a reasonable, risk-based sanctions compliance program, including SDN address screening of secondary market activity within its possession or control, satisfies its obligations under the rule, even if a blocked person it had no reasonable means to identify nonetheless transacts with its stablecoin. Finally, ADB asks the agencies to confirm that, in applying its Economic Sanctions Enforcement Guidelines to apparent violations arising from secondary market activity, OFAC will give substantial mitigating weight to the existence and adequacy of such a program, as the NPRM indicates.[13]

This clarification would directly answer the questions on which the agencies seek comment regarding the technical and operational challenges of implementing block, freeze, and reject capabilities for the secondary market, and would preserve the reasonable, risk-based character of

---

PPSIs must have technical capabilities, policies, and procedures "to identify and block stablecoins traded by blocked persons on the secondary market when PPSIs exercise possession or control of such stablecoins, including through smart contracts").

[10] Proposed 31 C.F.R. § 502.303; NPRM, 91 Fed. Reg. at 18,619.

[11] Proposed 31 C.F.R. § 502.201(b)(3); NPRM, 91 Fed. Reg. at 18,616-17.

[12] NPRM, 91 Fed. Reg. at 18,589.

[13] *Id.* at 18,589 (noting that, in applying its Economic Sanctions Enforcement Guidelines, 31 C.F.R. Part 501, App. A, "OFAC considers favorably the presence of an effective sanctions compliance program at the time of an apparent violation").

the regime while still achieving the agencies' national security objectives.

III. Application of the BSA to ADB as Both a Bank and a PPSI

Because ADB is an uninsured national bank, it would be subject to BSA obligations both as a bank under Part 1020 and as a PPSI under proposed Part 1033. The NPRM acknowledges that, where obligations differ, such an institution "will be required to comply with both sets of obligations," while expressing FinCEN's expectation that its efforts to harmonize obligations across financial institution types will allow efficient compliance.[14] FinCEN expressly requests comment on "whether it is proposing any obligations that would conflict with existing obligations such that complying with both would be legally or practically impossible."[15]

Based on its preliminary review, ADB has not identified any obligation in the proposed rule that conflicts with the obligations applicable to ADB as a bank such that complying with both would be legally or practically impossible. ADB notes that FinCEN has designed the proposed AML/CFT program for PPSIs to mirror, in substantial part, the program proposed for banks, which materially reduces the potential for conflict.[16] ADB offers two recommendations to give effect to FinCEN's harmonization objective.

First, FinCEN should confirm in the preamble to the final rule that an entity that is both an uninsured national bank and a PPSI may maintain a single, enterprise-wide AML/CFT program that satisfies both its Part 1020 and its Part 1033 obligations, paralleling the approach FinCEN describes for PPSIs that are subsidiaries of insured depository institutions, where an enterprise may extend a single program to both entities so long as the program is reasonably designed to identify and mitigate the risks of each entity's activities and satisfies each applicable requirement.[17] FinCEN should likewise confirm that, where a bank obligation and a PPSI obligation are parallel, an institution that complies with the more specific or more stringent of the two is deemed to satisfy both.

Second, ADB encourages FinCEN, OFAC, and the primary Federal payment stablecoin regulators to coordinate their respective examination, supervision, and enforcement activities, so that an institution subject to overlapping obligations is not subject to duplicative reviews or inconsistent supervisory expectations across agencies. Upon finalization of the rule, ADB intends to review its written policies and procedures, along with the regulatory citations within them, and to update them to reflect the final text. Clear preamble guidance confirming the foregoing would facilitate that exercise and promote the efficiencies the NPRM seeks.[18]

IV. Targeted Clarifications to the Proposed AML/CFT Program

---

[14] *Id*. at 18,591 ("Where obligations differ, an institution that is both a bank and a PPSI … will be required to comply with both sets of obligations.").

[15] *Id.* at 18,591-92; *see also id*. at 18,620 (Question 2).

[16] *Id.* at 18,591 (FinCEN "is proposing to impose an AML/CFT program on PPSIs that largely mirrors its proposed programs for banks").

[17] *Id.* at 18,591 (describing the use of a single, enterprise wide AML/CFT program and FinCEN's 2012 administrative ruling); *see* FinCEN, FIN-2012-R005 (Aug. 13, 2012).

[18] *Id.* at 18,592.

a. Examiner consideration of public blockchain data should remain risk-based and should not become a de facto secondary market monitoring obligation.

The NPRM states that, although a PPSI is not required to monitor secondary market activity, a PPSI "will be required to understand the risk its customers pose as part of its due diligence, as well as its distribution channels, including the blockchains on which its payment stablecoins are deployed," and the preamble observes that public blockchain data may inform a PPSI's development of a customer risk profile, for example where such data indicates that a customer exchange engages in deposit or withdrawal activity with addresses attributed to illicit actors.[19] ADB does not object to considering reasonably available public information in developing customer risk profiles, which is consistent with sound, risk-based due diligence. ADB requests, however, that FinCEN confirm in the final rule preamble that this expectation remains risk-based and proportionate, and that it does not, whether by rule or through examination expectations, convert the absence of a formal secondary market monitoring requirement into a de facto obligation to conduct transaction-level surveillance of downstream, secondary market activity. A clear statement to this effect would preserve the coherence of FinCEN's decision not to require secondary market monitoring and would give PPSIs and examiners a common, predictable understanding of the diligence expected.[20]

b. The risk assessment update trigger should remain principles-based, with clarification that routine technical deployments are not automatically "significant" changes.

Proposed § 1033.210(b)(1)(i)(C) would require a PPSI to update its risk assessment "promptly upon any change that the PPSI knows or has reason to know significantly changes its ML/TF risk profile," and the preamble identifies examples such as deploying a stablecoin on a new blockchain, coding new features into a smart contract, and adding new products or customer types.[21] ADB supports a principles-based, event-driven trigger and believes it is preferable to a fixed periodic schedule, because it focuses compliance resources on changes that actually affect risk.

Given the operational reality that a PPSI may deploy its stablecoin across multiple blockchains and update its smart contracts as a routine matter, however, ADB requests that FinCEN clarify, consistent with the question it has posed, that routine technical deployments or modifications that do not materially change a PPSI's ML/TF risk profile are not, standing alone, "significant" changes that automatically trigger a refreshed risk assessment, and that the reference to "distribution channels" is not intended to convert ordinary multi-chain availability into a continuous

[19] *Id*. at 18,592, 18,600-01 (although the proposed rule "would not impose a standalone, independent obligation on a PPSI to monitor secondary market transactions, consideration of such activity may be appropriate in the PPSI's development and maintenance of a customer risk profile," e.g., where "public blockchains may indicate that a digital assets exchange that is a PPSI customer is engaged in deposits or withdrawal activity of the PPSI's stablecoin with addresses attributed to illicit actors"); *see also id*. at 18,620 (Questions 8, 14, 17).

[20] *Id.* at 18,592 ("FinCEN is not proposing to require a PPSI as part of an AML/CFT program to monitor secondary market activity, although a PPSI will be required to understand the risk its customers pose as part of its due diligence, as well as its distribution channels, including the blockchains on which its payment stablecoins are deployed.").

[21] Proposed 31 C.F.R. § 1033.210(b)(1)(i)(C); NPRM, 91 Fed. Reg. at 18,600; *see also id.* at 18,599 (identifying "distribution channels," including "the blockchains to which its payment stablecoins are issued," as a risk assessment input under proposed § 1033.210(b)(1)(i)(A)).

reassessment obligation. ADB would not object to a "materially changes" formulation in place of "significantly changes" if FinCEN concludes it provides greater clarity. Either standard is workable provided the threshold is tied to genuine changes in the risk profile.[22]

V. Enhanced Due Diligence for Correspondent and Private Banking Accounts

Proposed § 1033.600 would apply most of the special standards of diligence in 31 C.F.R. Part 1010, subpart F to PPSIs, including enhanced due diligence for correspondent and private banking accounts,[23] and would amend the definition of "correspondent account" to include, as applied to a PPSI, "any formal relationship established by a permitted payment stablecoin issuer to provide regular services, dealings, and other financial transactions."[24]

ADB appreciates the clarity FinCEN provides and supports its decision not to apply § 1010.630 (the foreign shell bank prohibition) or § 1010.670 (foreign bank subpoena authority) to PPSIs, as well as its recognition that PPSIs remain subject to special measures under section 311 and related authorities.[25] ADB respectfully requests, however, that FinCEN confirm important limitations on the scope of the proposed correspondent account definition as applied to PPSIs.

Proposed § 1010.605(c)(2)(v) would define an "account," for correspondent account purposes, to reach "any formal relationship established by a [PPSI] to provide regular services, dealings, and other financial transactions," which the preamble describes as covering the full range of PPSI activities under 12 U.S.C. § 5903(a)(7). However, if read in isolation, that language could be understood to treat nearly every PPSI relationship as a correspondent account, vastly expanding the scope of enhanced due diligence requirements for PPSIs. Consistent with the statutory framework and with §§ 1010.610 and 1010.620, ADB respectfully requests that FinCEN clarify and confirm that the enhanced due diligence obligations still apply only to correspondent accounts established or maintained for foreign financial institutions and to private banking accounts for non-U.S. persons, and not to all primary market relationships of the PPSI.

VI. Sanctions Compliance Program Requirements

OFAC proposes to require PPSIs to maintain a sanctions compliance program containing five elements drawn from OFAC's 2019 Framework for OFAC Compliance Commitments: senior management and organizational commitment, risk assessment, internal controls, testing and auditing, and training.[26] ADB supports a risk-based program built around these five elements and welcomes OFAC's commitment to tailor the requirements to the size and complexity of each PPSI and to avoid a "one-size-fits-all" approach. ADB agrees that conducting a documented pre-launch BSA/AML and sanctions risk assessment before deploying a new stablecoin product or on a new

[22] NPRM, 91 Fed. Reg. at 18,620 (Question 15) (asking, among other things, whether "periodic updates or a set schedule for updates" would be preferable and whether a "materially changes" standard would "be clearer than 'significantly changes'").

[23] Proposed 31 C.F.R. § 1033.600; NPRM, 91 Fed. Reg. at 18,612-13.

[24] *Id.* at 18,612; proposed 31 C.F.R. § 1010.605(c)(2)(v).

[25] *Id.* at 18,612 (FinCEN "is not proposing to apply to PPSIs § 1010.630, which prohibits correspondent accounts for foreign shell banks, or § 1010.670, which relates to summons and subpoenas on foreign banks"); *see also id.* at 18,613 (special measures).

[26] Proposed 31 C.F.R. § 502.201(b)(1)-(5); NPRM, 91 Fed. Reg. at 18,614-19. The five elements are drawn from OFAC, *A Framework for OFAC Compliance Commitments* (May 2, 2019).

blockchain is sound practice, and ADB intends to continue to do so.

ADB asks only that OFAC confirm that the risk assessment element (including the expectation that risk assessments be conducted "at appropriate intervals" and revised to account for new products, services, mergers, or acquisitions) remains principles-based and does not impose a fixed cadence, consistent with OFAC's stated tailoring approach.[27] Finally, because the proposed internal controls element applies to "all payment stablecoin-related activity, whether on the primary or secondary market,"[28] the clarifications requested in Part II above are equally important here. The program should be measured against a reasonable, risk-based standard rather than treated as requiring a PPSI independently to identify every blocked person transacting in its stablecoin on the secondary market.

* * * * *

ADB believes that payment stablecoins issued by U.S.-based, regulated financial institutions can drive significant advances in payment and settlement technology while strengthening the integrity of the U.S. financial system. The NPRM is a thoughtful and substantial step toward an effective BSA and sanctions framework for PPSIs, and ADB generally supports its risk-based design and its careful treatment of the primary and secondary markets. With the targeted clarifications described above, the final rule can achieve the agencies' national security objectives while providing PPSIs the certainty needed to comply and to continue innovating responsibly.

ADB thanks FinCEN and OFAC for the opportunity to comment and looks forward to further engagement as the agencies finalize these important regulations.

Respectfully submitted,

/s/ Nathan McCauley

Nathan McCauley
Co-Founder, Chairman & Chief Executive Officer Anchorage Digital Bank NA

/s/ Rachel Anderika

Rachel Anderika
Chief Operating Officer & Chief Trust Officer
Anchorage Digital Bank NA

[27] *Id.* at 18,616; proposed 31 C.F.R. § 502.201(b)(2).

[28] Proposed 31 C.F.R. § 502.201(b)(3).

/s/ Dustin Palmer

Dustin Palmer
Bank Secrecy Act Officer
Anchorage Digital Bank NA