# Stablecoin Vendor Due Diligence Request List

## How to use this document

This is a 50-item request list designed to be sent verbatim to any stablecoin vendor your institution is evaluating. The list spans the four vendor archetypes a regional or community bank is likely to encounter: (1) payment stablecoin issuers, (2) custody and reserve-management providers, (3) on-ramp and off-ramp service providers, and (4) blockchain infrastructure providers (validator services, on-chain analytics, custody-as-a-service).

Each item is annotated with the regulatory anchor (where applicable), a one-line statement of what the reviewer is looking for, and a status column the vendor completes. The list maps to the five-document third-party risk management file structure every examiner expects: (a) board-approved risk appetite memo, (b) completed due diligence record, (c) executed contract and exhibits, (d) ongoing monitoring log, (e) tested termination plan. This document populates (b).

## Send the list under cover letter on bank letterhead. Set a response deadline (30 days is reasonable). Request that the vendor flag any item it considers confidential and propose a non-disclosure framework if needed. Document the back-and-forth in the vendor file.

## Section 1. Vendor identity and governance (Items 1-5)

**1. Legal entity structure.** Provide the full legal name of the contracting entity, state or country of formation, employer identification number (EIN) or equivalent foreign identifier, ownership structure including any parent and subsidiary entities, and an organizational chart showing entities that touch the service we are evaluating. *Reviewer is confirming: contracting counterparty matches the entity that holds the licenses and the reserves.*

**2. Beneficial ownership disclosure.** Identify every individual or entity holding 10 percent or more of voting equity or economic interest, consistent with FinCEN's beneficial ownership reporting standard under the Corporate Transparency Act of 2021, 31 U.S.C. § 5336. *Reviewer is confirming: no concentration of ownership in entities subject to sanctions or adverse regulatory action.*

**3. Board and senior management.** Provide names, titles, biographical summaries, and (for executives) regulatory disciplinary histories for the chief executive officer, chief financial officer, chief risk officer, chief compliance officer, chief information security officer, and the head of any function that touches

our service. *Reviewer is confirming: leadership has the depth and the regulatory track record to operate a regulated payments business.*

**4. Material litigation and regulatory actions.** List every material litigation matter, regulatory enforcement action, or supervisory consent order against the vendor or any affiliate within the past five years, whether resolved or pending. Include matters related to BSA/AML, OFAC, consumer protection, securities, commodities, and money transmission. *Reviewer is confirming: the vendor is not under an active order that constrains its ability to perform under our contract.*

**5. Material adverse changes since most recent audited statements.** Disclose any material change in financial condition, regulatory status, ownership, leadership, business model, or operations since the most recent audited financial statements. *Reviewer is confirming: the vendor file reflects current conditions, not a snapshot from 12 to 18 months ago.*

---

## Section 2. Regulatory status and licensing (Items 6-10)

**6. Charter or licensing posture.** Identify the charter or license under which the vendor operates the service we are evaluating: federal trust bank, state-chartered trust, money transmitter (state-by-state list), state qualified payment stablecoin issuer (QPSI) under GENIUS § 8, federal qualified payment stablecoin issuer (FQPSI) under GENIUS § 4, or other. *Reviewer is confirming: the vendor operates under a charter or license that authorizes the activity we are receiving.*

**7. State money transmitter license inventory.** Provide a current list of every state in which the vendor holds a money transmitter license, the license numbers, the state regulator points of contact, and the renewal dates. Identify any state where the vendor operates under an exemption rather than a license. *Reviewer is confirming: license coverage extends to every state in which our customers will use the service.*

**8. GENIUS Act compliance posture.** Confirm the vendor's status under GENIUS Act, Pub. L. No. 119-27 (July 18, 2025): (a) if a payment stablecoin issuer, identify the federal regulator and confirm § 4(a)(1)(A) full-reserve backing, § 4(a)(1)(B) maturity restriction, § 4(a)(11) yield prohibition, and § 4(a)(4) capital and liquidity standards; (b) if a digital-asset service provider, confirm compliance with CLARITY Act § 404 yield prohibition under the joint SEC, CFTC, and Treasury rulemaking framework. *Reviewer is confirming: the vendor's product structure does not depend on a yield model the statutes have closed.*

**9. CLARITY Act Title V activities (if vendor is a bank).** If the vendor is a depository institution or trust company providing services under CLARITY Title V (Bank Activities in Digital Assets), provide the supervisory non-objection or examination correspondence confirming the activity is permitted under the institution's charter. *Reviewer is confirming: bank-vendor counterparties are operating with their regulators' awareness of the activity.*

**10. FATF Travel Rule compliance.** Describe the vendor's compliance with the Financial Action Task Force Recommendation 16 (the Travel Rule) for virtual asset transfers above the $3,000 threshold under FinCEN regulations at 31 CFR § 1010.410(f). *Reviewer is confirming: cross-border stablecoin transfers carry originator and beneficiary information at the protocol layer.*

---

## Section 3. Reserves and redemption (Items 11-18)

This section applies to payment stablecoin issuers and reserve-management providers. Skip if the vendor is purely an infrastructure provider with no reserve responsibility.

**11. Reserve composition.** Provide the current composition of the reserve backing the stablecoin, by asset class and percentage: cash on deposit at qualified depository institutions, U.S. Treasury bills (maturity buckets), overnight repurchase agreements, government money market funds, and any other instrument. Confirm 1-for-1 backing under GENIUS § 4(a)(1)(A). *Reviewer is confirming: reserve composition complies with § 4(a)(1)(B) maturity restrictions (93 days or less) and § 4(a)(1)(C) eligible-asset definitions.*

**12. Bank counterparty list for reserve cash.** Identify every depository institution holding any portion of the cash component of the reserve, the percentage held at each, and the CAMELS-equivalent or supervisory rating of each (to the extent disclosed). *Reviewer is confirming: cash-deposit concentration risk is bounded, and the vendor has the capacity to add regional or community bank counterparties (Cross River, Customers, BNY Mellon, and others) or distribute through a reciprocal network (IntraFi ICS).*

**13. Treasury custodian and management arrangement.** Identify the custodian of the U.S. Treasury portion of the reserve, the asset manager (if separate), the custodial agreement structure, and the segregation arrangement (e.g., SEC-regulated registered investment company structure, trust account, or other). *Reviewer is confirming: reserve assets are held in a structure that survives the failure of the issuer or any service provider.*

**14. Third-party attestation cadence and standard.** Provide the most recent third-party attestation of reserve composition, the firm performing the attestation, the standard applied (AICPA 2025 Criteria for Stablecoin Reporting or equivalent), and the disclosed scope and limitations. *Reviewer is confirming: monthly attestation cadence is in place, the attestor is independent, and the standard applied has been examined and accepted by the issuer's regulator.*

**15. Public disclosure of reserve composition.** Provide the URL or platform where reserve composition is publicly disclosed and the disclosure cadence. Confirm consistency with GENIUS § 4(a)(10) standardized public-disclosure requirements. *Reviewer is confirming: the disclosure mechanism the customer-facing public sees matches the attestation in item 14.*

**16. Redemption mechanics and SLA.** Describe the customer-facing redemption mechanism: par-value redemption guarantee under GENIUS § 2(22)(A)(ii), redemption-procedure documentation under § 4(a)(1)(B), the redemption channel (issuer direct, exchange intermediated, both), the service-level commitment for time to settlement (T+0, T+1, T+2), and the customer-eligibility criteria. *Reviewer is confirming: end customers, not just exchange counterparties, have a credible redemption path at par.*

**17. Historical redemption stress events.** Describe every historical episode in which the issuer's stablecoin traded below par or experienced material redemption-fulfillment delay, including the March 10-13, 2023 USDC depeg episode (if applicable) and any subsequent event. Provide the issuer's post-event remediation report and the actions taken to address the root cause. *Reviewer is confirming: the vendor has a documented track record of operating through stress, not just through stable markets.*

**18. Reserve insurance and protections.** Identify any private insurance, performance bond, or third-party guarantee that backstops the reserve in the event of custodial loss, fraud, or operational failure.

Distinguish from FDIC coverage at the underlying depository institutions. *Reviewer is confirming: layered protections exist beyond the depository-institution-level FDIC coverage on the reserve cash component.*

---

## Section 4. Custody and key management (Items 19-23)

**19. Custody architecture.** Describe the custody architecture for any stablecoin or other digital asset the vendor holds on behalf of customers: hot wallet, warm wallet, cold storage allocation percentages, multi-signature (multisig) requirements, hardware security module (HSM) usage, and qualified-custodian status. *Reviewer is confirming: the vendor's custody design matches what a federally chartered trust bank (Anchorage, BitGo Trust) would implement.*

**20. Key generation and ceremony.** Describe the key generation ceremony, the threshold cryptography or multi-party computation (MPC) scheme in use, the number of co-signers required for transactions above defined thresholds, and the rotation and recovery procedures. *Reviewer is confirming: no single individual or single facility can move assets unilaterally.*

**21. Custody insurance.** Identify the carrier, policy limits, deductibles, coverage triggers, and exclusions for any insurance policy covering custodial loss. Provide a certificate of insurance. *Reviewer is confirming: insurance limits scale with the assets held and the exclusions do not vitiate the coverage.*

**22. Segregation of customer assets.** Confirm that customer assets are segregated from the vendor's proprietary assets, and that customer asset records distinguish the bank-customer's assets (where applicable) from those of other customers of the vendor. *Reviewer is confirming: in the event of vendor insolvency, customer assets are recoverable through a trust or bailment claim, not a general unsecured creditor claim.*

**23. Bankruptcy-remoteness opinion.** Provide a legal opinion from outside counsel addressing the bankruptcy-remoteness of customer assets held by the vendor under the relevant state or federal insolvency regime. *Reviewer is confirming: the legal theory supporting customer recovery has been independently reviewed and reduced to a written opinion.*

---

## Section 5. BSA, AML, OFAC, and sanctions (Items 24-29)

**24. BSA/AML program structure.** Provide the vendor's most recent independent BSA/AML program audit, the qualifications of the audit firm, the date of the audit, and the management response to any findings. Confirm program design consistent with FinCEN regulations at 31 CFR Chapter X. *Reviewer is confirming: the vendor has an examined and current BSA/AML program.*

**25. Customer identification program.** Describe the customer identification program (CIP) and customer due diligence (CDD) procedures, the data sources for identity verification, the politically-exposed-person (PEP) screening cadence, and the enhanced due diligence (EDD) triggers. *Reviewer is confirming: customer onboarding has the same rigor as a bank's CIP under 31 CFR § 1020.220.*

**26. Transaction monitoring on-chain.** Describe the on-chain transaction monitoring system, the analytics provider (Chainalysis, TRM Labs, Elliptic), the risk-typology coverage (mixers, sanctioned-

address attribution, ransomware payments, darknet markets), and the alert-disposition workflow. *Reviewer is confirming: the vendor monitors the on-chain leg of every transaction, not just the on-ramp fiat leg.*

**27. SAR and CTR filing posture.** Provide aggregate SAR and CTR filing statistics for the most recent 12 months, the average time from event to filing, and the procedures for sharing case data with the bank's BSA officer. *Reviewer is confirming: filing posture is consistent with the volume and risk profile of the activity.*

**28. OFAC sanctions screening.** Describe the OFAC screening procedure for both customer identities and on-chain wallet addresses, the screening cadence (real-time vs. periodic), the source of the sanctioned-address list (OFAC's Specially Designated Nationals (SDN) list plus secondary attribution data), and the freeze-and-report procedure on a positive hit. *Reviewer is confirming: the screening covers both the customer layer and the wallet-address layer, and the freeze procedure is operationally tested.*

**29. FinCEN MSB or money transmitter examination history.** Provide the most recent FinCEN BSA examination report (if applicable) and any state money-transmitter examination reports from the prior 24 months. Confirm any open matters requiring attention (MRAs) or matters requiring immediate attention (MRIAs). *Reviewer is confirming: regulator-visible compliance gaps are disclosed before the bank decides to engage.*

---

## Section 6. Technology and blockchain operations (Items 30-34)

**30. Network deployment list.** Identify every blockchain network on which the vendor's stablecoin is deployed or the vendor's service operates: Ethereum mainnet, Ethereum Layer-2s (Base, Arbitrum, Optimism), Solana, Polygon, Avalanche, Stellar, and others. Identify the smart contract addresses for each. *Reviewer is confirming: deployment surface area is known, and the vendor has not deployed to networks the bank's risk appetite does not cover.*

**31. Smart contract audit history.** Provide the audit history of every smart contract supporting the service: audit firm, date, scope, findings, and remediation. Confirm independent audit consistent with vendor's regulator's expectations. *Reviewer is confirming: smart contract code has been independently reviewed by qualified firms (Trail of Bits, OpenZeppelin, ConsenSys Diligence, CertiK, Halborn).*

**32. Network upgrade and fork procedures.** Describe the procedure for responding to network upgrades, hard forks, and contentious protocol changes on each deployed network. Identify governance participation rights and historical voting positions. *Reviewer is confirming: the vendor has a documented decision framework for upgrade events, not an ad-hoc response.*

**33. Validator and node infrastructure (if applicable).** If the vendor operates validator nodes on proof-of-stake networks, identify the networks, the operating model (in-house vs. white-label through Figment, Blockdaemon, Kiln, or Coinbase Cloud), the slashing-insurance arrangement, and the historical slashing-event record. *Reviewer is confirming: validator operations are governed by the standard described in OCC IL 1174, 1183, and 1184.*

**34. System availability and reliability.** Provide the past 24 months of uptime and incident statistics for the customer-facing service, the largest single outage, and the post-incident review. *Reviewer is confirming: operational reliability supports the service-level commitments in the contract.*

---

## Section 7. Cybersecurity and incident response (Items 35-38)

**35. Cybersecurity program framework.** Identify the cybersecurity framework the vendor follows (NIST CSF 2.0, ISO 27001, SOC 2 Type II) and provide the most recent third-party attestation under that framework. *Reviewer is confirming: an independent third party has examined the vendor's cyber program against a recognized standard.*

**36. Penetration testing cadence and scope.** Describe the penetration testing program: cadence, scope (network, application, smart contract, social engineering), test firm, methodology, and the disposition of critical and high findings. *Reviewer is confirming: testing is regular, broad, and remediated under a tracked timeline.*

**37. Incident response and notification.** Provide the incident response plan and confirm the customer-notification timing for security incidents that affect customer funds, customer data, or service availability. Confirm consistency with the FDIC, OCC, and Federal Reserve's 36-hour computer-security incident notification rule (12 CFR Part 304, Subpart D and parallel agency rules, effective May 2022). *Reviewer is confirming: the bank will be notified inside the 36-hour window when an incident affects the service we receive.*

**38. Historical security incidents.** Disclose every material security incident in the past five years, including any incident reportable under the 36-hour rule, any successful intrusion, any customer fund loss, and any data breach. Provide the post-incident remediation summary for each. *Reviewer is confirming: the vendor's historical track record is known before the contract is signed, not after the first incident.*

---

## Section 8. Fourth-party and subservicer risk (Items 39-42)

In the bank-fintech partnership context, the term "fourth party" describes a fintech partner's downstream service providers. The same logic applies to a stablecoin vendor: the bank's fourth parties are the vendor's vendors.

**39. Critical fourth-party inventory.** Provide a list of every fourth-party service provider whose failure would materially affect the service we receive, including custodians, audit firms, blockchain infrastructure providers, banking partners, and cloud providers. *Reviewer is confirming: the dependency chain is documented and the bank can assess concentration risk across the chain.*

**40. Fourth-party diligence and monitoring program.** Describe the vendor's own third-party risk-management program, including the standard against which fourth parties are diligenced (FFIEC interagency third-party risk-management guidance, June 6, 2023) and the monitoring cadence. *Reviewer is confirming: the vendor diligences its own vendors with the same rigor we are applying to the vendor.*

**41. Right to audit fourth parties.** Confirm the bank's right under the master services agreement to audit (directly or through a designated agent) any fourth party whose failure would affect the service we receive, subject to commercially reasonable notice and confidentiality. *Reviewer is confirming: the contractual right to inspect the dependency chain is not blocked by the vendor's own agreements.*

**42. Concentration risk in fourth parties.** Identify any fourth party that supports more than 25 percent of the vendor's customer base or more than $1 billion in transaction volume annually, and describe the concentration-risk mitigation in place. *Reviewer is confirming: a single fourth-party failure does not propagate through the entire stablecoin ecosystem.*

---

## Section 9. Financial strength and audit (Items 43-46)

**43. Audited financial statements.** Provide the most recent two years of audited financial statements, the auditor of record, and any going-concern or material-weakness commentary. *Reviewer is confirming: financial condition supports the contractual obligations the vendor is undertaking.*

**44. Capital adequacy.** Confirm capital adequacy consistent with GENIUS § 4(a)(4) (for issuers) or the equivalent regulator-imposed capital standard. Provide the most recent regulatory capital calculation and the buffer above the minimum. *Reviewer is confirming: the vendor is not operating at the regulatory floor.*

**45. Insurance coverage summary.** Provide a summary of every material insurance policy: directors and officers, errors and omissions, cyber, fidelity bond, custody, business interruption. Identify carriers, limits, and deductibles. *Reviewer is confirming: insurance is in place where contractual or statutory commitments require it.*

**46. Going-concern and operational continuity planning.** Provide the most recent business continuity and disaster recovery plan, the date of the most recent tabletop or live exercise, and the recovery time and recovery point objectives. *Reviewer is confirming: the vendor can continue to operate, or wind down in an orderly way, under a range of stress scenarios.*

---

## Section 10. Contractual provisions and termination (Items 47-50)

**47. Termination rights and procedures.** Confirm the bank's right to terminate the master services agreement upon (a) material breach, (b) regulator-directed termination, (c) the vendor's loss of any material license or charter, and (d) the bank's voluntary exit on commercially reasonable notice. Confirm the post-termination data-extraction procedure and the timeline. *Reviewer is confirming: the termination provisions match the five-document examiner expectation, including a tested termination plan.*

**48. Data ownership and portability.** Confirm that the bank owns the customer data, transaction records, and audit trail generated under the contract, and that the vendor will provide all such data in a machine-readable format on termination or at any time on request. *Reviewer is confirming: the bank can satisfy its record-retention obligations after the relationship ends.*

**49. Indemnification and limitation of liability.** Identify the indemnification provisions (covering at minimum: regulatory enforcement based on vendor breach, intellectual property infringement, data breach, and third-party claims arising from vendor service), and the limitation-of-liability cap. Confirm the cap is commercially reasonable in relation to the volume of activity contemplated. *Reviewer is confirming: the contract allocates risk in a way the bank's general counsel would accept on an unrelated commercial contract.*

**50. Examiner access.** Confirm the bank's regulators have direct access to the vendor's books, records, and operations relevant to the service we receive, consistent with the Bank Service Company Act, 12 U.S.C. § 1867(c), and the FFIEC interagency third-party risk-management guidance. *Reviewer is confirming: examiners can examine the vendor on the bank's behalf without requiring a separate vendor cooperation.*

---

## Submission and scoring

Return this completed document to the requesting institution by [DATE]. Flag any item the vendor considers confidential; the institution will execute a non-disclosure agreement if needed. Items the vendor declines to answer, or answers materially incompletely, will be tracked in the vendor file and reviewed at the bank's next vendor management committee meeting.

The bank's vendor management committee will score the completed DDQ on a four-point scale: (1) meets, (2) partial, (3) deficient, (4) declined. Any item scored deficient or declined requires either remediation by the vendor, a documented mitigant on the bank's side, or a board-level acceptance of the residual risk before the relationship moves to contract execution.

---

## Citations


[1] GENIUS Act, Pub. L. No. 119-27, July 18, 2025, § 2(22), § 4(a)(1)(A), § 4(a)(1)(B), § 4(a)(1)(C), § 4(a)(4), § 4(a)(10), § 4(a)(11), § 8.

[2] CLARITY Act, draft, Title V (Bank Activities in Digital Assets), Senate Banking Committee, May 2026.

[3] OCC Interpretive Letter 1172, January 4, 2021 (stablecoin reserve holding).

[4] OCC Interpretive Letter 1174, January 4, 2021 (validator node operations and stablecoin payment activities).

[5] OCC Interpretive Letter 1183, November 18, 2021.

[6] OCC Interpretive Letter 1184, March 7, 2025 (removal of supervisory non-objection requirement).

[7] FinCEN, Bank Secrecy Act regulations, 31 CFR Chapter X (BSA program, CIP, CDD, SAR/CTR filing).

[8] Financial Action Task Force, Recommendation 16 (Travel Rule), as implemented by FinCEN at 31 CFR § 1010.410(f).

[9] FinCEN, Corporate Transparency Act of 2021, 31 U.S.C. § 5336 (beneficial ownership reporting).

[10] FDIC, OCC, Federal Reserve, Computer-Security Incident Notification Rule, 12 CFR Part 304 Subpart D and parallel agency rules, effective May 1, 2022, with compliance from April 1, 2022.

[11] FFIEC member agencies, Interagency Guidance on Third-Party Relationships: Risk Management, June 6, 2023.

[12] Bank Service Company Act, 12 U.S.C. § 1867(c) (regulator access to bank service company books and records).

[13] American Institute of Certified Public Accountants, 2025 Criteria for Stablecoin Reporting: Specific to Asset-Backed Fiat-Pegged Tokens, 2025.

[14] Cong, L. W., "Stablecoins and Banking: Deposit Dynamics, Financial Stability, and Regulatory Design," Working Paper, December 7, 2025 (USDC reserve composition data, footnote 37).

[15] Federal Reserve Board, withdrawal of SR 22-6 and related interagency joint statements on crypto-asset risks, April 24, 2025.

[16] FDIC, FIL-7-2025, "Withdrawal of FIL-16-2022," March 28, 2025.

---

*Hickory and Company. AI Lab for Regulated Industries. Built so your board can defend it and your regulators can validate it.*