Spica Tech LLC

Enterprise AML/CFT & Sanctions (OFAC) Compliance Program

Version: 1.0

Date: October 20, 2024

Approved by: Board of Directors of Spica Tech LLC

BSA/AML Compliance Officer: Adriana Marcela Barrero (Administrator).

Scope: Global, with emphasis on operations subject to U.S. jurisdiction.

---

1. Purpose and Scope Statement

Spica Tech LLC ("Spica Tech" or the "Company") adopts this Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Compliance Program and Sanctions Compliance Program (OFAC) to prevent, detect, and mitigate financial crime risks across all business lines and in dealings with customers, vendors, partners, agents, and other third parties.

This Program is aligned with the FATF 40 Recommendations and the U.S. framework (BSA/AML, USA PATRIOT Act, AMLA 2020) as well as applicable OFAC sanctions programs and sectoral rules.

Applicability note. Certain obligations (e.g., CTR/SAR filings, the "Travel Rule") apply only to financial institutions as defined under the BSA (e.g., Money Services Businesses – MSBs, banks, brokers, etc.). Accordingly, this Program sets out:

a) Baseline controls mandatory for Spica Tech as a commercial enterprise when it is not acting as an FI/MSB; and

b) Enhanced controls and reporting that become active if and when Spica Tech qualifies as an FI/MSB (see Appendix G).

The BSA/AML Officer, in consultation with Legal, assesses applicability on an ongoing basis.

---

2. Key Definitions (excerpt)

- BSA/AML: Bank Secrecy Act and implementing regulations issued by FinCEN/U.S. Treasury.
- OFAC: Office of Foreign Assets Control (sanctions and blocking programs).
- BOI/CTA: Corporate Transparency Act beneficial ownership information reporting for Spica Tech and affiliates, where applicable.
- CDD/CIP: Customer Due Diligence / Customer Identification Program.
- PEP: Politically Exposed Person.
- MSB: Money Services Business (money transmission, currency exchange, etc.).
- Cash transactions: operations conducted with physical currency.

(Full glossary in Appendix A.)

---

3. Compliance Governance

3.1 Tone from the Top

The Board and Senior Management endorse this Program, allocate sufficient resources (human, technological, and budgetary), and adopt a zero-tolerance stance toward non-compliance.

3.2 Roles and Responsibilities

- Board of Directors: approves the Program; reviews metrics and the annual AML/CFT report.
- BSA/AML Officer: designs, implements, and maintains the Program; serves as primary liaison with banks, FinCEN/OFAC (as applicable), and auditors; coordinates investigations, reporting, and training.
- Line-of-Business Leaders: implement operational controls; validate product/market risks.
- Technology & Data: ensure data integrity, auditability, and security.
- All Employees: comply with policies, report red flags, and complete training.

3.3 Independence and Resourcing

The BSA/AML Officer reports to the Board or Audit Committee with authority to escalate and to halt high-risk activity.

---

4. Risk-Based Approach (RBA)

4.1 Risk Assessment Methodology

Spica Tech performs an enterprise AML/CFT risk assessment annually (and ad hoc upon material change) covering:

- Customer/counterparty risk (type, geography, PEP exposure, history).
- Product/service risk (payments, refunds, credit, prepaids, crypto if applicable).
- Geographic risk (sanctioned/high-risk jurisdictions).

- Channel risk (non-face-to-face, agents/third parties, marketplaces).
- Transaction risk (amounts, patterns, cash, cross-border transfers).

A scoring model (low/medium/high) with a risk matrix and mitigation plan is used (see Appendix B). Results are reported to the Board.

4.2 Risk Acceptance and Escalation

- Low/Medium risk: mitigate via standard controls.
- High risk: requires Enhanced Due Diligence (EDD) and BSA/AML Officer approval; document rationale and implement heightened monitoring.

---

5. Know Your Customer and Third Parties (KYC/CDD/CIP)

While statutory CIP applies to banks and certain FIs, Spica Tech adopts functionally equivalent procedures as best practice and to meet banking/partner expectations.

5.1 Onboarding of Natural Persons

- Minimum data: full name, date of birth, nationality, residential address, valid government ID; document/electronic verification.
- Checks: sanctions/PEP screening, adverse media, geographic coherence.

5.2 Onboarding of Legal Entities

- Data: legal name, registered address, jurisdiction of incorporation, registration number, purpose, ownership structure and beneficial owners (≥25% or control); TIN/EIN or equivalent.
- Beneficial Ownership Declaration signed by an authorized representative.
- Checks: sanctions/PEP screening of owners/controllers; adverse media; required licenses.

5.3 Higher-Risk Customers/Third Parties (EDD)

EDD is required for PEPs, high-risk/sanctioned geographies, complex ownership structures, agents/intermediaries, or products with higher anonymity. Measures include sources of wealth/funds, bank references, virtual/on-site meeting, reinforced limits, and senior approval.

5.4 Refresh and Remediation

KYC data are refreshed based on risk (e.g., every 1–3 years), and immediately upon trigger events (activity spikes, ownership changes, negative alerts).

———————————————————————————————

6. Sanctions (OFAC) & Geofencing Controls

6.1 Principles

Spica Tech maintains a Sanctions Compliance Program proportionate to its risk built on:

- Senior management commitment.
- Sanctions risk assessment.
- Documented internal controls.
- Independent testing/audit.
- Ongoing training.

6.2 Lists and Scope

Screening is performed against:

- OFAC SDN List and other applicable lists (e.g., SSI, CAPTA, program-specific lists).
- 50 Percent Rule: entities owned (directly or indirectly, in aggregate) ≥50% by a blocked person are considered blocked.

6.3 Handling Potential Matches

- True hits: block or reject as applicable; freeze assets where required and report to OFAC within 10 business days; retain records; manage licenses if needed.
- False positives: document analysis and release.
- Uncertain cases: escalate to BSA/AML Officer and Legal; do not process until resolved.

6.4 Technical Controls

- Screening at onboarding, upon data changes, and real-time for payments/receipts.
- Geofencing (IP/origin/delivery country), blocking sanctioned countries/programs; anti-evasion controls (re-exports, trans-shipments, fronts).
- Sanctions evasion detection: structuring/fragmentation, intermediaries, routing changes, atypical logistics/packaging to conceal origin/destination.

---

7. Transaction Monitoring & Alerts

7.1 Approach

Risk-based monitoring with scenarios and thresholds tailored to Spica Tech's business (purchases, refunds, transfers, cash where applicable, crypto if applicable).

7.2 Indicators & Typologies (examples)

- Activity inconsistent with customer profile (volumes, frequency, spikes).
- Structuring/smurfing or circular flows.
- High-risk/sanctioned jurisdictions without legitimate purpose.
- Third parties are not reasonably connected; sudden beneficiary changes.
- Mismatch between declared source of funds and observed activity.
- Fraud typologies: pig-butchering, TBML, use of CVC kiosks (if applicable).

7.3 Alert Handling & Investigations

- Risk-based prioritization; resolution SLAs and quality KQIs.
- Case files with chronology, evidence, analysis, and disposition (close, EDD, escalate).
- Record retention for ≥5 years.

---

8. Regulatory Reports & Thresholds (only if Spica Tech is an FI/MSB)

Applies only if Spica Tech becomes subject to FI obligations (e.g., MSB registration). Otherwise, Spica Tech does not file CTRs/SARs but escalates to its banks/partners and authorities where appropriate (see §9).

8.1 Suspicious Activity Reports (SARs)

- MSBs: file SARs for suspicious activity ≥ USD 2,000 (typical deadline: 30 days from detection; extendable if subject cannot be identified).
- Tipping-off prohibition applies.

8.2 Currency Transaction Reports (CTRs)

- FI obligation for cash transactions > USD 10,000 in a single business day (deposits/withdrawals/other).
- Aggregation by person/day; anti-structuring controls.

8.3 Funds Transfer Recordkeeping / "Travel Rule"

- Transmittals of funds ≥ USD 3,000: retain and transmit required originator/beneficiary data to the next financial institution, per applicable rules.
- Special rules for cross-border transfers; retain records ≥5 years.

8.4 Recordkeeping & Retention

- Retain most BSA/AML records for 5 years (policies, reports, evidence, alerts/investigations, KYC, transfers).

---

9. Escalation to Banking Partners & Authorities (when Spica Tech is not an FI/MSB)

- Banks/partners: if Spica Tech identifies activity that may constitute financial crime, escalate to acquiring bank/payment processor for their SAR/CTR evaluation.
- Authorities: upon reasonable suspicion of serious crimes (fraud, extortion, trafficking, sanctions violations), consult Legal regarding reporting/cooperation.
- Retention: document internal assessments, decisions, and evidence for ≥5 years.

---

10. Product Change & Project Governance

Prior to launching new products/markets/channels, Spica Tech will perform a product sanctions & AML/CFT risk assessment (e.g., cross-border payments, wallets, crypto, vouchers, agents), defining:

- Inherent risk, mitigating controls, pilots, limits, monitoring metrics.
- Local regulatory requirements (if any) and supplier contracts (AML/OFAC clauses, audit rights, termination for breach).

---

11. Third Parties, Agents & Vendors

Spica Tech applies KYS/KYTP (Know Your Supplier/Third Party):

- Risk-proportionate due diligence (identity, beneficial owners, sanctions, reputation, licenses, adverse history).
- Contracts with AML/OFAC clauses (compliance, audit trial, cooperation, incident reporting, termination rights).
- Ongoing monitoring: adverse media alerts, corporate changes, control effectiveness.

———————————————————————————————

12. Privacy & Information Security

- Data processing in accordance with applicable laws (U.S. and, where relevant, GDPR).
- Data minimization, access controls, encryption in transit/at rest, limited retention.
- Immutable audit logs for AML/CFT and sanctions decisions.

———————————————————————————————

13. Training & Awareness

- Onboarding and annual mandatory training for all personnel; enhanced modules for higher-risk teams (Sales, Support, Finance, IT).
- Core topics: business-specific AML/CFT risks, OFAC sanctions, red flags, escalation procedures, confidentiality, case studies.
- Effectiveness: testing, completion metrics, surveys, workshops.

———————————————————————————————

14. Independent Testing/Audit

- Frequency: at least annually (risk-based) by Internal Audit or an independent third party.
- Scope: governance, RBA, KYC, sanctions, monitoring, investigations, reporting (if applicable), recordkeeping, data integrity, stress testing.
- Findings must have remediation plans tracked to closure.

———————————————————————————————

15. Communication, Documentation & Retention

- Formal player retentionand Board aapproval. Minimum 5-year retention of policies, KYC records, alyear retentiontions, decisions, evidence, audit results, and reports (as applicable).
- Central repository with access control and audit trail.

———————————————————————————————

16. Whistleblower & Non-Retaliation

Confidential channels (email/phone) are available to report suspected financial misconduct. No retaliation is tolerated; Compliance and Legal investigate all cases.

———————————————————————————————

17. Red-Flag Indicators – Operational Guide

Non-exhaustive; to be used alongside FinCEN/FFIEC typologies and current advisories:

- Structuring to evade thresholds or screening.
- Multiple refunds to unrelated third parties.
- Unusual use of custodians/intermediaries without clear business logic.
- Payments to/from high-risk or sanctioned jurisdictions.
- Discrepancies between KYC and transactional behavior.
- Use of CVC with poor traceability; mixers/tumblers; kiosks.

- Fraud indicators: social engineering, unrealistic “investment” schemes, romance scams, “tech support” scams.

Action: pause the activity, analyze, request additional information, escalate to the BSA/AML Officer, and document the decision.

---

18. Corporate Transparency Act (CTA) – BOI (for Spica Tech)

Applies to Spica Tech itself (not to its customers) if it qualifies as a “reporting company” under the CTA.

- Internal Owner: Corporate Secretary or Corporate Legal.
- Timing/Events: submit initial BOI and update upon changes (ownership/control, BO data, company data) pper currentdedeadlines; etain evidence of filings.
- Contents: beneficial owners (≥25% or substantial control) and company applicants (as applicable).
- Coordination: align with internal KYC and provide to banks upon request.

---

19. Incident Management & Government Interaction

- Documented process to respond to legal requests: Section 314(a) information-sharing (for banks, if interposed), subpoenas, court orders, and NSLs (through Legal).
- Evidence preservation and chain of custody.
- Logs of communications, decisions, and legal advice.

---

20. Complementary Statements

- Anti-Bribery/ABC: separate but coordinated policies (FCPA and local laws).
- Fraud: prevention and response program aligned with AML/CFT.
- Ethics & Sustainability: commitment to lawful, transparent business.

---

21. Approval, Effectiveness & Review

This Program becomes effective as of the date above and will be reviewed at least annually or upon material changes in business, regulation, or risk profile.

Appendices

Appendix A. Glossary (excerpt)

Beneficial owner: natural person with ≥25% ownership or substantial control.

Established customer: ongoing relationship with KYC completed.

EDD: enhanced due diligence measures.

MSB: FI category covering money transmitters, currency exchangers, issuers/sellers of monetary instruments, etc.

PEP: senior public function holder (and close associates/family).

SDN: entities/persons designated by OFAC.

Appendix B. Risk Assessment Template (summary)

- Factors: customer (type, PEP, BO, history), product/service, geography, channel, transactions.
- Matrix: likelihood × impact; inherent/residual; mitigating controls.
- Action plan: owners, deadlines, metrics.

Appendix C. KYC Requirements (checklists)

Natural people:

- Valid government ID; proof of address; selfie/video-KYC (if used); sources of income (if EDD).

Legal entities:

- Formation documents; certificate of good standing; BO declaration; org chart; board resolution for account/relationship; licenses.

Screening: sanctions, PEP, adverse media; country risk.

Appendix D. Sanctions Handbook (operational summary)

1) Screening onboarding and ongoing; 2) 50 Percent Rule; 3) Alert handling (investigation, block/reject, 10-business-day report); 4) Licenses; 5) Periodic testing (lists & engine); 6) Specialized training.

Appendix E. SAR Decision Matrix (conditional – FI/MSB)

- Triggers: typologies, thresholds, events (fraud, sanctions, TBML, CVC).

- **Deadlines:** 30 days from detection (extend to 60 if subject unknown).
- **Narrative:** clear write-up using FinCEN terms; supporting exhibits.

Appendix F. Record Retention (minimums)

- KYC/EDD, alerts, cases, reports (if any), audits: **≥5 years.**
- Sanctions screening logs and block/reject records: **≥5 years.**

Appendix G. MSB/FI Addendum (active only if Spica Tech qualifies as FI/MSB)

G.1 AML Program – Four Pillars: written internal controls; designated BSA Officer; ongoing training; independent testing (annual).

G.2 SARs (MSB): file for ≥ USD 2,000 suspicious activity; 30-day deadline (60 if subject unknown); confidentiality/no tipping-off.

G.3 CTRs (MSB/Banks): report cash > USD 10,000 per day; anti-structuring; 5-year retention.

G.4 Recordkeeping/Travel Rule: ≥ USD 3,000 transmittals; retain and transmit required data; 5-year records.

G.5 MSB Registration: register with FinCEN (if applicable); maintain evidence for 5 years; agent oversight.

G.6 Section 314(b) (voluntary for FIs): annual notice to FinCEN to share information with other FIs; confidentiality and permitted-use controls.

G.7 CVC/Crypto (if applicable): assess money transmitter status; Travel Rule; state licensing (where required); crypto-specific red flags.

Appendix H. CTA – BOI (for Spica Tech)

- Status: determine whether Spica Tech (and subsidiaries) is a "reporting company."
- Deadlines: comply with current BOI filing/update timelines.
- Data: BOs (≥25% or control), applicants (as applicable), address, TIN/EIN, accepted IDs.
- Governance: owner, quality controls, evidence archive, request handling.

Appendix I. Training Curriculum

- Overview of BSA/AMLA/OFAC/FATF.
- KYC/CDD/EDD (individuals and entities).
- Sanctions (50 Percent Rule, blocks/rejects, 10-day reports).
- Monitoring & red flags (fraud, TBML, CVC, scams).
- Investigations, documentation, narrative.
- Privacy/security, ethics, conflicts of interest.

Appendix J. Documentation & Evidence Inventory

- Current policies and procedures; risk reports; list versions; QA/QC results; remediation plans; training evidence.

Appendix K. Corporate Data (completed)

- Legal name: Spica Tech LLC
- EIN: 37-2144528

- Registered address: 1007 North Orange Street, 4th Floor, Wilmington, Delaware 19801, USA
- Telephone: +54 911 3560 0328 (Administrator)

———————————————————————————————

Legal disclaimer. This Program does not constitute legal advice. Regulatory references are subject to change. Spica Tech will review and update the Program to reflect regulatory, interpretive, or business model changes. For specific matters, consult qualified counsel.

———————————

Administrator Signature

Adriana Marcela Barrero