Anti-Money Laundering (AML) & Know Your Customer (KYC) Policy

AI Trade Flow — Advanced Education and Trading

Effective Date: [DATE] · Last Updated: [DATE]

1. Statement of Commitment

AI Trade Flow LLC is committed to preventing its Services from being used for money laundering, terrorist financing, sanctions evasion, fraud, or any other financial crime. Although AI Trade Flow does not accept deposits, hold customer funds, or transmit money — all trading occurs in accounts our members own at third-party exchanges — we voluntarily maintain this program as a matter of good governance and to support the compliance obligations of our payment processors and members' exchanges.

2. Relationship to the Bank Secrecy Act (BSA) and FinCEN Standards

AI Trade Flow is not a bank, money services business, money transmitter, broker-dealer, or other "financial institution" as defined under the Bank Secrecy Act (31 U.S.C. § 5311 et seq.), because it never takes custody of, transmits, or exchanges funds or digital assets. Accordingly, formal BSA obligations — FinCEN registration, Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and the Customer Identification Program rules of the USA PATRIOT Act — attach to our members' exchanges and our payment processors, not to AI Trade Flow directly.

We nonetheless structure this program voluntarily around the BSA's five-pillar AML program standard: (1) written internal policies, procedures, and controls (this Policy); (2) a designated Compliance Officer accountable for the program; (3) ongoing employee training; (4) periodic independent review of the program's effectiveness; and (5) risk-based customer due diligence, including identity verification and ongoing monitoring. Where our BSA-regulated partners — payment processors and members' exchanges — request information in support of their own BSA/AML obligations, including SAR investigations, we cooperate promptly and fully within the limits of applicable privacy law. If our services ever change in a way that brings AI Trade Flow within the BSA's definitions, we will register and implement the corresponding formal program before offering those services.

3. Scope

This Policy applies to all AI Trade Flow members, employees, contractors, and officers, and covers membership onboarding, subscription payments, account linking, and ongoing use of the Services.

4. Know Your Customer (KYC)

Before or shortly after activating a membership, and always before enabling account-linking features, members may be required to provide: full legal name; date of birth; residential address; country of citizenship and residence; and a government-issued photo ID verified through our third-party identity-verification vendor. We may request updated or additional documentation at any time, and we may suspend access while verification is pending or unresolved.

5. Sanctions and Watchlist Screening

Members are screened at onboarding and periodically thereafter against applicable lists, including the U.S. Treasury OFAC Specially Designated Nationals (SDN) list and other government sanctions and watchlists. We do not provide Services to: persons or entities on such lists; residents of comprehensively sanctioned jurisdictions; or anyone whose use of the Services would cause us or our vendors to violate applicable law.

6. Prohibited Conduct

Members may not: use the Services in connection with proceeds of crime; pay membership fees using stolen, unauthorized, or anonymized payment instruments; create accounts under false identities or on behalf of undisclosed third parties; use the Services to structure, layer, or conceal the movement of funds; or engage in market manipulation, including wash trading and coordinated pump-and-dump activity.

7. Digital-Asset Payments — Screening and Merchant Status

Membership charges may be paid in supported digital assets, and program payouts may be delivered the same way. Accepting crypto as payment for our own services, and paying our own contractual obligations in crypto, is merchant ("user") activity under FinCEN guidance — not money transmission — and does not alter Section 2's analysis; we reassess this position before any change to how funds flow. Crypto payments are accepted only after KYC verification and only to unique addresses generated in the member-portal checkout and controlled by the company. Card-funded payments flow through an independent, licensed onramp provider that applies its own KYC, sanctions screening, and card-network controls to the fiat-to-crypto conversion before the asset reaches our checkout address. Source wallets are screened against OFAC-listed addresses and blockchain-analytics risk indicators, and we refuse — and may return to the originating address after review — payments associated with sanctioned addresses, mixers or tumblers, privacy-enhanced obfuscation, darknet markets, or known proceeds of crime. Payouts are made only to wallet addresses verified by the recipient member, are screened before release, and are reported for tax purposes at their U.S. dollar value on the payout date.

8. Monitoring and Red Flags

We monitor for indicators including: mismatches between billing identity and verified identity; repeated failed verification attempts; use of high-risk or anonymizing payment methods; logins from sanctioned or high-risk jurisdictions; multiple memberships tied to one payment source; and reports from members' exchanges or our payment processors. Red flags trigger review by the Compliance Officer and may result in requests for information, suspension, or termination.

9. Reporting and Cooperation

Where required or appropriate under applicable law, we will report suspicious activity to competent authorities and will cooperate with lawful requests from law enforcement and regulators. Members will not be notified of reports where notification is prohibited ("no tipping off").

10. Record Keeping

Verification records, screening results, and related compliance documentation are retained for at least five (5) years after account closure, or longer where law requires, consistent with our Privacy Policy.

11. Governance and Training

The designated Compliance Officer ([NAME/TITLE], compliance@[DOMAIN]) owns this Policy, reviews it at least annually, and oversees staff training on recognizing and escalating suspicious activity. This Policy may be updated as regulations, guidance, and our Services evolve.

12. Member Acknowledgment

By using the Services, you agree to provide accurate verification information, to keep it current, and to comply with this Policy. Failure to complete verification, or conduct that violates this Policy, may result in suspension or termination without refund, to the extent permitted by the Refund & Cancellation Policy and applicable law.

This document is a template prepared for AI Trade Flow and must be reviewed by qualified legal counsel before publication or use.