

VALUE BRIDGE SINGLE MEMBER INVESTMENT SERVICES S.A.

AML, CTF AND SANCTIONS STATEMENT

Last updated: 30th of June 2026

Important notice. This public Statement summarises the high-level Value Bridge's approach to anti-money laundering, counter-terrorist financing, sanctions, fraud prevention, and financial crime controls for its Crypto-Asset Services.

1. Introduction and Regulatory Status

1.1. Value Bridge Single Member Investment Services S.A. is a Greek investment services firm authorised and regulated by the Hellenic Capital Market Commission (HCMC) under the Markets in Financial Instruments framework and Law 4514/2018, which transposed Directive 2014/65/EU on markets in financial instruments into Greek law.

1.2. Value Bridge's HCMC license number is 6/927/31-8-2021. Value Bridge is registered in Greece under GEMI with register number 161690660000. Its registered office is at 43 Aioulou Street, 3rd floor, 10551 Athens, Greece.

1.3. Value Bridge has submitted a notification to HCMC under Article 60 of Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA), Protocol No. 8101. The relevant crypto-asset service is the reception and transmission of orders for crypto-assets on behalf of clients.

1.4. Value Bridge does not operate a crypto-asset trading platform, does not provide custody of crypto-assets, does not operate clients' wallets, does not control clients' private keys, does not issue crypto-assets, does not provide crypto payment processing services, and does not provide merchant settlement services.

1.5. Value Bridge is committed to preventing the misuse of its Services for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, tax evasion, bribery, corruption, market abuse, or other unlawful activity.

1.6. Value Bridge applies anti-money laundering, counter-terrorist financing, sanctions, and financial crime controls in accordance with Applicable Law, HCMC expectations, internal policies, and the risk-based approach.

2. Risk-Based Approach

2.1. Value Bridge applies a risk-based approach to clients, beneficial owners, authorised representatives, transactions, payment methods, crypto-assets, jurisdictions, wallets, Third-Party Venues, and transaction routes.

2.2. Risk factors may include client type, geography, source of funds, source of wealth, transaction size, transaction frequency, payment method, wallet screening result, blockchain analytics, sanctions exposure, adverse media, PEP status, delivery channel and other relevant information.

2.3. Enhanced measures may be applied where a higher risk is identified.

3. Client Identification and Verification

3.1. Value Bridge may identify and verify the identity of natural persons using reliable and independent information, documents, or data.

3.2. For legal entities, Value Bridge may collect and verify information concerning the entity's name, legal form, registered office, directors, authorised representatives, beneficial owners, ownership and control structure, and powers to bind the entity.

3.3. Value Bridge may refuse to provide Services unless it is satisfied with the identification, verification, ownership, control, authority, and risk profile of the client and relevant persons.

3.4. Value Bridge may request additional information or documents at any point before, during, or after the processing of a Client Order where required or considered appropriate.

4. Beneficial Ownership and Authorised Representatives

- 4.1. Value Bridge seeks to identify the beneficial ownership of legal entity clients and to understand the ownership and control structure of such clients.
- 4.2. Value Bridge may verify that any person purporting to act on behalf of a client is duly authorised and may identify and verify such person.
- 4.3. Where Value Bridge cannot establish beneficial ownership, control, authority, or the purpose and nature of the relationship or transaction to its satisfaction, it may reject onboarding, refuse a Client Order, suspend processing, or terminate the relationship.

5. PEP, Sanctions and Adverse Media Screening

- 5.1. Value Bridge applies screening measures for sanctions, politically exposed persons, adverse media, and other financial crime indicators.
- 5.2. Where a client or beneficial owner is identified as a politically exposed person, Value Bridge may apply enhanced due diligence, obtain senior management approval where required, establish source of funds and source of wealth, and conduct enhanced monitoring.
- 5.3. Value Bridge will not knowingly establish or maintain a relationship or process a transaction that would breach applicable sanctions or other legal restrictions.

6. Source of Funds, Source of Wealth and Transaction Purpose

- 6.1. Value Bridge may request information and documentation concerning source of funds, source of wealth, purpose and nature of the transaction, expected activity, payment method, and economic rationale.
- 6.2. Value Bridge does not knowingly accept funds or crypto-assets where there is reasonable cause to believe that they may have been acquired illegally, represent proceeds of crime, or are connected with unlawful activity.
- 6.3. Value Bridge does not accept cash deposits or deposits using cash-related methods in connection with the Crypto-Asset Services.

7. Wallet Screening and Transaction Monitoring

- 7.1. Value Bridge may screen clients' wallets, wallet addresses, blockchain transaction information, and transaction routes using internal systems and external blockchain analytics providers.
- 7.2. Value Bridge may monitor transactions before, during, and after processing to identify unusual, suspicious, high-risk, prohibited, or non-compliant activity.
- 7.3. Wallet addresses or transaction routes may be rejected, suspended, delayed, or subject to additional checks where they present sanctions, AML/CTF, fraud, darknet market, scam, mixing, tumbling, ransomware, stolen funds, prohibited jurisdiction, or other risk indicators.

8. Travel Rule and Information Sharing

- 8.1. Value Bridge may be required to collect, verify, retain, transmit, or receive originator and beneficiary information in accordance with Travel Rule, AML/CTF, sanctions, tax, or other regulatory requirements.
- 8.2. Value Bridge may share relevant information with Third-Party Venues, payment providers, banks, compliance providers, regulators, financial intelligence units, courts, law enforcement agencies, auditors, advisers, or other parties where required or permitted by Applicable Law.
- 8.3. A User must provide all information required for compliance with Travel Rule and related requirements. Failure to provide such information may result in rejection, suspension, cancellation, delay, or termination.

9. Suspicious Activity Reporting and Recordkeeping

- 9.1. Where Value Bridge suspects money laundering, terrorist financing, sanctions evasion, fraud, or other unlawful activity, it may submit reports to the competent authorities in accordance with Applicable Law.

9.2. Value Bridge may be restricted from informing a User about certain reports, investigations, or actions where disclosure would be unlawful or inappropriate.

9.3. Value Bridge maintains records of client identification, verification, due diligence, transactions, screening, monitoring, internal reports, and reports to authorities in accordance with Applicable Law and internal policies.

10. Refusal, Suspension and Termination

10.1. Value Bridge may reject onboarding, refuse a Client Order, delay processing, request additional information, restrict functionality, suspend access, terminate a relationship, or take other measures where required or considered appropriate for AML/CTF, sanctions, fraud prevention, legal, regulatory, or risk reasons.

10.2. Value Bridge may take such measures without prior notice where prior notice would be unlawful, compromise controls, create risk, or be inconsistent with regulatory or third-party requirements.

11. Contact

11.1. For compliance and onboarding enquiries, Users may contact compliance@valuebridge.global.