

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING COMPLIANCE AGREEMENT

Section 1.1: Purpose, Scope, and Regulatory Alignment

This Anti-Money Laundering and Counter-Terrorist Financing Compliance Agreement (the “**AML/CTF Agreement**”) forms part of the contractual documentation governing the Customer’s access to and use of the Company’s Services.

The purpose of this AML/CTF Agreement is to establish the requirements, controls, and procedures applied by the Company to protect its Services and operations against money laundering, terrorist financing, fraud, tax-related offenses, misappropriation of assets, sanctions violations, proliferation financing, and other unlawful or prohibited conduct.

The Company is committed to conducting its Services for legitimate purposes and in accordance with Applicable Law, applicable anti-money laundering (“**AML**”) and counter-terrorist financing (“**CTF**”) requirements, regulatory standards, and applicable compliance obligations.

The Customer acknowledges that compliance with the Company's AML and CTF requirements is a condition of accessing and continuing to use the Services.

Section 1.2: Legal Compliance and Regulatory Cooperation

1.2.1 Financial Crime Prevention

The Company maintains a zero-tolerance approach toward money laundering, terrorist financing, fraud, sanctions violations, and other financial crime.



Where the Company identifies or reasonably suspects activity that may involve unlawful conduct, the Company may undertake appropriate compliance measures, including enhanced review, transaction restriction, account restriction, suspension, or termination, subject to Applicable Law.

1.2.2 Regulatory and Law Enforcement Cooperation

The Company may cooperate with competent authorities, regulators, law enforcement agencies, financial intelligence units, supervisory bodies, payment providers, and other legally authorized entities in connection with AML, CTF, sanctions, financial crime prevention, or other lawful investigations.

Such cooperation may include the disclosure of Customer information, transaction records, account information, communications, or other relevant records where required or permitted by Applicable Law.

The Company may make such disclosures without prior notice to the Customer where notification is prohibited, not legally required, or could prejudice an investigation or compliance obligation.

Section 1.3: Customer Identification and Due Diligence

1.3.1 Identity Verification

As a condition of accessing the Services, the Customer may be required to undergo identity verification in accordance with the Company's Know Your Customer (“KYC”) procedures and Applicable Law.

The Company may establish and verify the Customer's identity before establishing a business relationship, providing particular Services, processing transactions, or continuing the Customer relationship.

1.3.2 Verification Requirements

The Customer shall provide complete, accurate, current, and verifiable information and documentation requested by the Company for identification, verification, compliance, and risk-assessment purposes.

The Company may request additional information or documentation where reasonably necessary to satisfy its AML, CTF, sanctions, fraud-prevention, or other compliance obligations.

1.3.3 Failure to Complete Verification

Failure to complete required verification procedures or maintain accurate and current information may result in restrictions on the Customer Account, refusal or delay of transactions, suspension of Services, or termination of the Customer relationship.

Section 1.4: Source of Funds and Economic Purpose

1.4.1 Source of Funds

The Customer shall provide information concerning the lawful origin of funds deposited, transferred, or otherwise used through the Services where requested by the Company.

The Company may require supporting documentation to verify the source of funds, source of wealth, ownership of funds, or other information relevant to the legitimacy of a transaction.

1.4.2 Economic Purpose and Transaction Rationale



The Company may request information concerning the purpose, nature, or economic rationale of particular transactions where reasonably necessary for compliance, risk assessment, or financial crime prevention.

The Customer shall cooperate with such requests and provide accurate and sufficient information within the timeframe reasonably specified by the Company.

1.4.3 Access to Compliance Records

The Company may retain transaction, verification, and compliance records in accordance with Applicable Law.

The Company may restrict disclosure of such records where disclosure could compromise regulatory obligations, an investigation, security measures, crime-prevention efforts, or the rights of another person.

Section 1.5: Recordkeeping and Regulatory Reporting

1.5.1 Compliance Records

The Company, directly or through appointed service providers, may maintain records relating to Customer identification, verification, transactions, communications, compliance reviews, risk assessments, and other relevant information for the periods required by Applicable Law.

1.5.2 Suspicious Activity Reporting

Where the Company identifies activity that it reasonably considers suspicious or potentially connected to money laundering, terrorist financing, sanctions violations,



fraud, or other unlawful activity, it may submit Suspicious Transaction Reports (“**STRs**”), Suspicious Activity Reports (“**SARs**”), or equivalent reports to competent authorities.

The Company may make such reports without notifying the Customer where required or permitted by Applicable Law.

The Company shall not be required to disclose the existence, contents, or status of any such report where disclosure is prohibited or restricted by Applicable Law.

Section 1.6: Internal Controls, Risk Assessment, and Enhanced Due Diligence

1.6.1 Compliance Controls

The Company maintains internal governance mechanisms, compliance procedures, monitoring systems, risk controls, and review processes designed to identify, assess, and mitigate AML and CTF risks.

These controls may include transaction monitoring, Customer risk profiling, sanctions screening, identity verification, source-of-funds checks, enhanced review, and other measures appropriate to the nature and level of identified risk.

1.6.2 Higher-Risk Customers and Activities

The Company may apply enhanced scrutiny to Customers, transactions, activities, or relationships presenting increased financial crime risk.

Such circumstances may include relationships involving Politically Exposed Persons (“**PEPs**”), higher-risk jurisdictions, unusual transaction patterns, complex ownership structures, or other indicators identified through the Company's risk-assessment procedures.

1.6.3 Risk-Based Due Diligence

Customer due diligence shall be applied on a risk-sensitive basis.

Depending on the circumstances and Applicable Law, the Company may apply simplified, standard, or enhanced due diligence measures.

Enhanced due diligence may include:

- (a) additional identification or verification documents;
- (b) source-of-funds or source-of-wealth information;
- (c) additional transaction information;
- (d) transaction limits or restrictions;
- (e) intensified monitoring;
- (f) independent verification from external sources; or
- (g) other measures reasonably necessary to manage identified risks.

Section 1.7: Third-Party Representation and Authorized Persons

1.7.1 Authorized Representatives

The Company does not establish or maintain relationships with anonymous or unidentified persons.

Where a third party seeks to act on behalf of a Customer, the Company may require a valid power of attorney, identification documents, authorization records, and other supporting documentation before permitting the third party to act.

1.7.2 Verification of Authority

The Company may independently verify the identity and authority of any person acting on behalf of a Customer.

The Company may reject, suspend, or restrict a transaction or instruction where the relevant authorization, identity, or compliance requirements have not been satisfactorily established.

Section 1.8: Refusal, Restriction, and Termination

The Company may refuse to process a transaction or may restrict, suspend, or terminate the Customer relationship where:

- (a) the Customer fails to provide requested information or documentation;
- (b) information provided by the Customer is false, misleading, incomplete, or inconsistent;
- (c) the Customer fails to satisfy applicable KYC, AML, CTF, or sanctions requirements;
- (d) activity is inconsistent with the Customer's declared purpose or known profile;
- (e) the Company identifies or reasonably suspects unlawful or prohibited activity;
- (f) the Company is unable to complete required compliance procedures; or
- (g) such action is reasonably necessary to satisfy Applicable Law or a requirement of a competent authority.

Such measures may be implemented without prior notice where immediate action is reasonably necessary to satisfy legal, regulatory, security, or financial crime prevention obligations.

Section 1.9: Customer Risk Profiling and Financial Crime Indicators

1.9.1 Risk Assessment Factors

When assessing AML and CTF risk, the Company may consider a range of factors, including, without limitation:

- (a) the Customer's legal status, ownership structure, and control arrangements;

- (b) transaction patterns, frequency, size, and volume;
- (c) geographic exposure and jurisdictional connections;
- (d) the nature of the Customer's business or activities;
- (e) counterparties and transaction relationships;
- (f) source of funds and source of wealth information;
- (g) sanctions or adverse information identified through screening; and
- (h) other factors relevant to financial crime risk.

1.9.2 Financial Crime Indicators

Where indicators suggest potential links to illicit activity, sanctions violations, terrorist financing, proliferation financing, fraud, or other prohibited conduct, the Company may apply enhanced controls, restrict activity, suspend Services, or terminate the Customer relationship, subject to Applicable Law.

Section 1.10: Uniform Application of Compliance Requirements

The Company's AML, CTF, KYC, sanctions, and related compliance procedures shall apply without improper discrimination or exemption based on personal relationships, referrals, commercial arrangements, internal affiliations, or other non-compliance-related considerations.

No Customer shall be exempt from mandatory verification, due diligence, sanctions screening, or other legally required compliance measures.

The Company may apply additional requirements where the relevant Customer, transaction, jurisdiction, or activity presents increased risk.

Section 1.11: Legal Capacity and Eligibility



Where concerns arise regarding a Customer's legal capacity, identity, authority, eligibility, or ability to lawfully access the Services, the Company may require additional documentation or verification before permitting continued access.

The Company may suspend or restrict the Services while such matters are being assessed.

Where the Company reasonably determines that the Customer is legally ineligible to access the Services or that the relevant relationship cannot lawfully continue, the Company may discontinue the relationship in accordance with the Customer Terms of Use and Applicable Law.

Section 1.12: Continuous Monitoring and Compliance Review

Customer information, account activity, and transactional behavior may be subject to ongoing monitoring throughout the duration of the Customer relationship.

The Company may periodically review and update Customer risk profiles based on changes in Customer information, transaction behavior, applicable regulatory requirements, emerging financial crime typologies, or other relevant risk factors.

The Company may request updated information or documentation at any time where reasonably necessary to maintain accurate Customer records or satisfy its ongoing compliance obligations.

Section 1.13: Customer Cooperation Obligations

The Customer shall cooperate fully with AML, CTF, KYC, sanctions, and other financial crime prevention measures implemented by the Company.

The Customer shall:

- (a) respond promptly to reasonable requests for information or documentation;
- (b) provide accurate, complete, and current information;
- (c) provide supporting documentation where reasonably required;
- (d) notify the Company of material changes to information previously provided where required; and
- (e) comply with applicable verification and compliance procedures.

Failure to cooperate may result in transaction restrictions, account restrictions, suspension, or termination of the Customer relationship.

Section 1.14: Compliance Measures and Protective Actions

The Company may implement any reasonable compliance or protective measure necessary to manage identified AML, CTF, sanctions, fraud, or other financial crime risks, subject to Applicable Law.

Such measures may include transaction holds, payment restrictions, enhanced verification, additional monitoring, account restrictions, suspension of Services, refusal of transactions, or termination of the Customer relationship.

The Company shall not be required to disclose internal monitoring methods, risk indicators, investigative procedures, or other confidential compliance information where disclosure could compromise the effectiveness of its controls or violate Applicable Law.

Section 1.15: Amendments and Ongoing Compliance Governance

The Company may amend, update, replace, or supplement this AML/CTF Agreement from time to time to reflect changes in Applicable Law, regulatory expectations, financial crime risks, internal risk assessments, compliance procedures, or operational requirements.



An updated version may be published through the Official Website, Customer Portal, Platform, or another Official Communication Channel designated by the Company.

Unless otherwise required by Applicable Law, an amendment shall become effective on the date specified by the Company or, where no date is specified, upon publication.

The Customer's continued use of the Services following the effective date of an amendment constitutes acknowledgement of the updated AML/CTF Agreement, subject to any rights that cannot lawfully be excluded.