AML/KYC POLICY

Having regard for the safety of the users and due to the legal requirements, The European Union, The Unity States of America and other countries, zam.io has implemented and started to use this AML/KYC policy (customer's identification), AML / CTF (combating money-laundering and terrorist financing) as it is required from banks and other financial institutions.

The purpose of those policies is an effective combating of money-laundering and terrorist financing (AML / CTF) on our website by proper identification of actual users of our accounts and supervision of their transactions. We shall identify and cease transactions made not only to purchase/sell a cryptocurrency but made mainly to hide the criminal origin of money, finance illegal activity or other unlawful behaviors.

Specific provisions of our policies are confidential and for internal use only, in order to prevent their avoidance by dishonest or fraudulent users. We would like to introduce to you some of the general rules and stipulations of our policies which directly concern you and affect the services we render.

Money Laundering is conducting or attempting to conduct a financial transaction knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activities. We, zam.io, have developed this Anti-Money Laundering Compliance and Know your Client Policy ("AML/KYC Policy") in an effort to maintain the highest possible compliance with applicable laws and regulations relating to anti-money laundering in in any jurisdictions, where we conduct business.

Internal Controls

We have developed robust internal policies, procedures, and controls designed to comply with applicable laws and regulations, as well as any other reporting requirements and audits.

Legal Compliance Officer

Our Legal Compliance Officer ("LCO") is responsible for developing and enforcing the policies and procedures of our AML Policy. Our LCO is required to report any violations of our AML Policy directly to our CEO. In addition, our LCO is responsible for recording and filing SARs, CTRs and performing an AML Policy audit at least annually.

Customer Identification

Our Customer Identity Program ("CIP") is an important part of our AML Policy, and helps us detect suspicious activity in a timely manner and prevent fraud.

Account Opening Process

In order to open an account and use zam.io, your identity must be verified, authenticated, and checked against government watchlists, including the Office of Foreign Assets Control ("OFAC"). Failure to complete any of these steps will result in your inability to use zam.io.

Individual customer — Prior to opening an account for an individual customer, we attempt to collect, verify, and authenticate the following information:

- Full and correct name of person;
- Permanent address;
- Email address;
- Nationality;
- Mobile phone number;
- Social Security Number ("SSN") or any comparable identification number issued by

government;
- Date and place of birth ("DOB");
- Proof of identity: copy of first four pages of passport (e.g., driver's license, or government-issued ID), showing the following details: (a) number and country of issuance, (b) issue and expiry date, (c) signature of the person;
- Additional information or documentation at the discretion of our Compliance Team.

If you successfully meet and complete our CIP requirements and do not appear on the OFAC or any other government watchlist, then we will provide you with account opening agreements electronically.

Institutional customer — Prior to opening an account for an institutional customer, we attempt to collect, verify, and authenticate the following information:

- Institution legal name;
- Employer Identification Number ("EIN") or any comparable identification number issued by government;
- Full legal name (of all account signatories and beneficial owners);
- Email address (of all account signatories);
- Mobile phone number (of all account signatories);
- Address (principal place of business and/or other physical location);
- Proof of legal existence (e.g., state certified articles of incorporation or certificate of formation, certified copy of the Memorandum and Articles of Association, location of registered office, proof of good standing, unexpired government-issued business license, trust instrument or other comparable legal documents as applicable);
- Contract information of owners, principals, and executive management (as applicable);
- Proof of identity (e.g., driver's license, passport or government-issued ID) for each individual beneficial owner that owns 10% or more, as well as all account signatories; and
- Identifying information for each entity beneficial owner that owns 10% or more (see individual customer information collected above for more details).

If your institution successfully meets and completes our CIP requirements and neither it nor any of its owners, principals, executive, or managers appear on OFAC or any other governmental watchlist, we will provide you with account opening agreements electronically.

Suspicious Activity/Currency Transaction Reports Opening Process

We file SARs if we know, suspect or have reason to suspect suspicious activities have occurred on zam.io. A suspicious transaction is often one that is inconsistent with a customer's known and legitimate business, personal activities or personal means. We leverage our compliance department, which performs transaction monitoring to help identify unusual patterns of customeractivity. Our LCO reviews and investigates suspicious activity to determine if sufficient information has been collected to justify the filing of a SAR.

Our LCO maintains records and supporting documentation of all SARs and CTRs that have been filed.

Reporting Requirements

All records are retained for seven (7) years and are readily available upon official request by an applicable examiner, regulator, or law enforcement agency.

AML Policy Audit

- Internal

The LCO is responsible for performing an audit of our AML Policy at least annually and presenting the results to our CEO.

- Independent

Our CEO oversees the performance of an independent test of our AML Policy at least annually. The LCO is not responsible for the independent test, and the LCO's performance is a subject of the test. Results are sent directly to the CEO for review.

Transactions' monitoring and supervision

Using our proprietary software we also analyse all transactions that take place on our website looking for suspicious and unusual behaviours. Such selected transactions are analysed by our AML specialists and evaluated if they do not provide significant AML / CTF risks or if they needed to be ceased and clarified with the User.

Additional verification

When your trade volume rises, our AML / CTF verification duties increase as well. The same happens when your transactions are "flagged" as suspicious or unusual, or our verification of your personal results in qualifying you as a person imposing significant AML / CTF risk.

In such cases, we can require additional documentation proving your real, exact place of residence, education, occupation, as well as the source of money you are using on our website.

Unfortunately, if our LCO or any other AML professional decide information received from you do not clarify our doubts, we will be obliged to end our cooperation with you or even report your transactions to relevant authorities.

Restricted Jurisdictions

In accordance with our policies we do not open accounts and do not process transactions for citizens and residents of, as well as people staying in, countries where transactions are prohibited by international sanctions or their internal law regulations, or countries which based on various criteria selected by our AML team (for example Corruption Perceptions Index by Transparency International, FATF warnings, countries with weak anti-money laundering and terrorist financing regimes determined by European Commission) impose high AML / CTF high risk.

Currently, these countries are Afghanistan, American Samoa, Angola, Bahamas, Botswana, Burundi, Cambodia, Central African Republic, Chad, Congo, Cuba, Democratic Republic of Congo, Equatorial Guinea, Eritrea, Ethiopia, Ghana, Guam, Guinea Bissau, Iran, Iraq, North Korea, Lebanon, Libya, Mali, Nigeria, Pakistan, Panama, Puerto Rico, Samoa, Saudi Arabia, Sierra Leone, Somalia, South Sudan, Sri Lanka, Sudan, Syria, Trinidad and Tobago, Tunisia, Venezuela, Yemen, Zimbabwe, USA (citizens and residents).

Tiers of KYC verification

When your trade volume rise AML / CTF risk increases as well. That is why we have to introduce proper safety and verification procedures. As a result, we introduced three Tier verification system, based on the general rule that the more money (or cryptocurrencies) you deposit or want to withdraw the more information about you and your funds we need to exclude AML / CTF risks (as we are required by law).

You should remember that this model is a result of the work and experience of our AML team and can be changed as the legal requirements of countries changes as well as a result of gaining new knowledge and experience. In particular transition, limits may change due to periodical audits and verification of efficiency of our procedures. We will keep you updated if any changes would influence your situation.