Introduction

Blue Diamond's Anti-Money Laundering and Know Your Customer Policy (hereinafter - the "AML/KYC Policy") is designated to prevent and mitigate possible risks of BLUE DIAMOND being involved in any kind of illegal activity.

Both international and local regulations require BLUE DIAMOND to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity from its Users.

AML/KYC Policy covers the following matters:

- Verification procedures.
- Compliance Officer.
- Monitoring Transactions.
- Risk Assessment.

1. Verification procedures

One of the international standards for preventing illegal activity is customer due diligence ("CDD"). According to CDD, BLUE DIAMOND establishes its own verification procedures within the standards of anti-money laundering and "Know Your Customer" frameworks.

1.1. Identity verification

BLUE DIAMOND S's identity verification procedure requires the User to provide BLUE DIAMOND S with reliable, independent source documents, data or information (e.g., national ID, international passport, bank statement, utility bill). For such purposes BLUE DIAMOND reserves the right to collect User's identification information for the AML/KYC Policy purposes.

BLUE DIAMOND will take steps to confirm the authenticity of documents and information provided by the Users. All legal methods for double-checking identification information will be used and BLUE DIAMOND reserves the right to investigate certain Users who have been determined to be risky or suspicious.

BLUE DIAMOND S reserves the right to verify User's identity in an on-going basis, especially when their identification information has been changed or their activity seemed to be suspicious (unusual for the particular User). In addition, BLUE DIAMOND reserves the right to request up-to-date documents from the Users, even though they have passed identity verification in the past.

User's identification information will be collected, stored, shared and protected strictly in accordance with the BLUE DIAMOND's Privacy Policy and related regulations.

Once the User's identity has been verified, BLUE DIAMOND is able to remove itself from potential legal liability in a situation where its Services are used to conduct illegal activity.

1.2. Card verification

The Users who are intended to use payment cards in connection with the BLUE DIAMOND's Services have to pass card verification in accordance with instructions available on the BLUE DIAMOND's Site.

2. Compliance Officer

The Compliance Officer is the person, duly authorized by BLUE DIAMOND, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of BLUE DIAMOND's anti-money laundering and counter-terrorist financing, including but not limited to:

a. Collecting Users' identification information.

b. Establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations.

c. Monitoring transactions and investigating any significant deviations from normal activity.

d. Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs.

e. Updating risk assessment regularly.

f. Providing law enforcement with information as required under the applicable laws and regulations.

The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activity.

3. Monitoring Transactions

The Users are known not only by verifying their identity (who they are) but, more importantly, by analyzing their transactional patterns (what they do). Therefore, BLUE DIAMOND relies on data analysis as a risk-assessment and suspicion detection tool. BLUE DIAMOND performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting. System functionalities include:

1) Daily check of Users against recognized "black lists" (e.g. OFAC), aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;

2) Case and document management.

With regard to the AML/KYC Policy, BLUE DIAMOND will monitor all transactions and it reserves the right to:

- ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
- request the User to provide any additional information and documents in case of suspicious transactions;

- suspend or terminate User’s Account when BLUE DIAMOND has reasonably suspicion that such User engaged in illegal activity.

The above list is not exhaustive and the Compliance Officer will monitor Users transactions on a day-to-day basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide.

4. Risk Assessment

BLUE DIAMOND, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, BLUE DIAMOND is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

Timely reaction to “Red Flags” and other signs of suspicious customer behavior. All non-trading financial transactions are tested for money laundering for all stages of cash flow in money laundering:

 Accommodation. At this stage, funds are converted to other financial instruments such as checks, bank accounts, money transfers, or they can be used to purchase expensive goods that can be resold. They can also be invested in banks. and non-banking institutions (for example, currency exchange offices). To avoid suspicion from parties to the company, the money launderer may spend several investments instead of order to invest the entire amount at once. This form of placement is called “stumping” or "spray".
 Splitting up. Funds are transferred or transferred to other accounts and other financial instruments. This is done in order to hide the origin and prevent identification a person who has carried out several financial transactions. Moving and reshaping cash complicates the process of tracking laundered money.
 Integration. The funds are returned to circulation as legally received for the purchase of goods and services.

After evaluating these risks, each risk category is evaluated on a three-point scale:

 Low risk. There are no risk factors in each category, customer operations are transparent and do not have deviations from normal operations; sensible person doing business in appropriate areas. Thus, there is no reason to suspect that risk factors in general may lead to to the threat of money laundering or terrorist financing
 Medium risk. One risk factor or several risk factors in categories that differ from normal operations of a person who does business in the relevant field, but operations are still transparent. Thus, there is no reason to suspect that risk factors can generally cause a threat money laundering or terrorist financing
 High risk. One feature or several traits in categories that generally undermine transparency of the face and its operations, as a result of which these faces differ from the face working in the relevant field. Thus, the risk of money laundering or terrorist financing The company reserves the right to collect additional customer identification data. for AML / KYC policy. The data and documents used to identify the client by the Company will be collected, be stored, shared and protected strictly in accordance with the provisions of the Law on Counteracting legalization (laundering) of criminally obtained incomes and the

financing of terrorism in accordance with the Company's internal privacy policy and applicable governing to the principles.

5. Data Protection Officer.

Our Data Protection Officer is the person in charge of ensuring our company adheres to this privacy policy. This person is also the main contact for our Data Protection Supervisory Authority, the Information Commissioner’s Office. The Data Protection Officer may be contacted on support@crypto1.io

Data Protection Supervisory Authority

Our Data Protection Supervisory Authority in terms of data protection is the Estonian National Data Protection Authority. You may contact the authority at support@crypto1.io if you wish to discuss with them any instance where you feel we may not be adhering to the terms within this Privacy Policy or to raise a complaint.