AML

FEB 2024

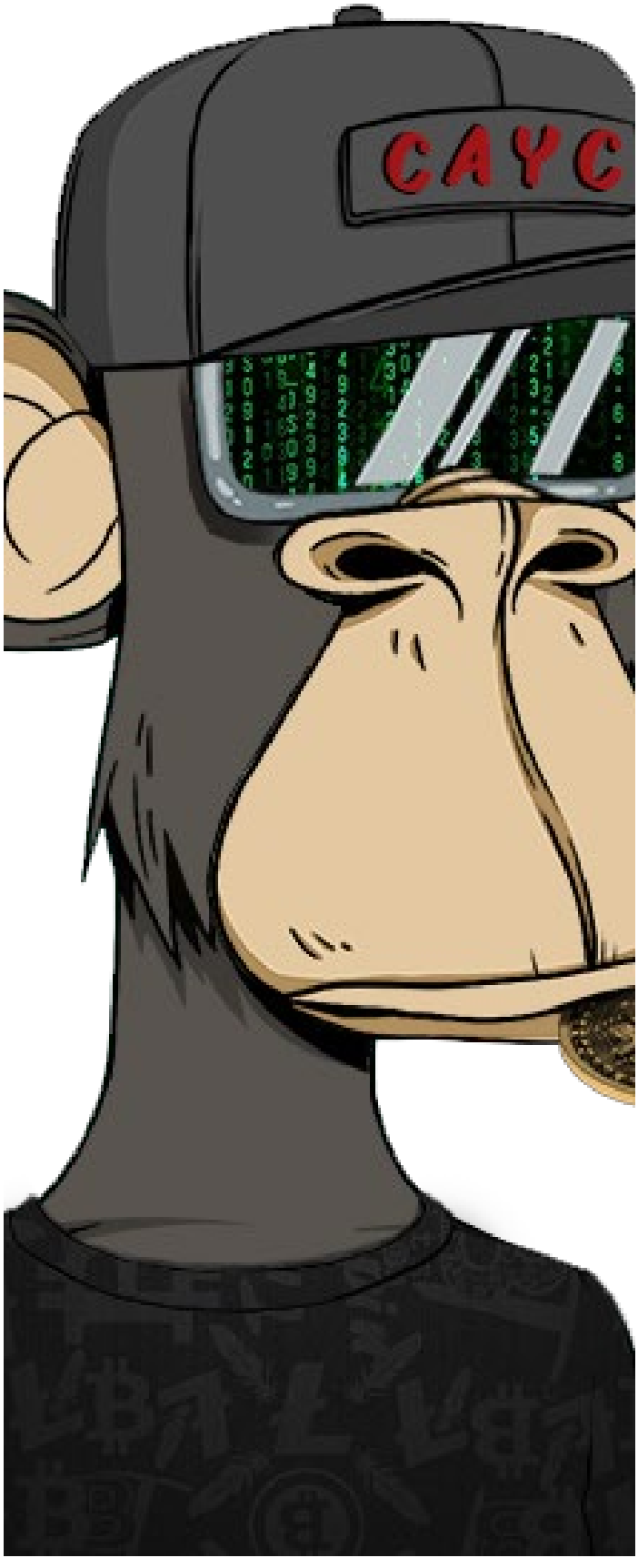

Table of Contents

Anti-Money Laundering, Anti-Terrorist Financing statement

1. Company Business Model

CYBER APES YACHT CLUB ("CAYC" or the "Company") is a brand name of EIGHT GALAXIES LIMITED, a Company incorporated in Cyprus under Registration no. HE 438664 and having its Registered Office at Avlonos 1, MARIA HOUSE, 1075 Nicosia, Cyprus and has established compliance measures commensurate with its services and products that are reasonably designed to deter and detect illicit activity on its platform. Such measures include onboarding and compliance screenings of its customers and transaction action-based controls.

2. Company Policy Statement

CAYC is not a financial institution and is accordingly not directly subject to the statutes and regulations applicable to certain financial institutions, money transfer, or virtual asset service providers. However, in accordance with the 2016 Regulations for Anti-Money Laundering and Combating the Financing of Terrorism ("AML**/CFT**") CAYC expressly prohibits and rejects the use of CAYC products for any form of illicit activity, including money laundering, terrorist financing or trade sanctions violations, consistent with various national anti-money laundering ("**AML**") laws, regulations, and norms. CAYC continues to monitor norm setting parameters promulgated by the Financial Action Task Force ("**FATF**") and certain gaming trade groups and will take necessary action as it deems appropriate to reflect changes in law.

CAYC's intention is to follow global best practices in guarding against CAYC products being used to facilitate such activities. Those best practices include:

- Adoption of a written policy, and procedures and controls, reasonably designed to guard against money laundering, terrorist financing and trade sanctions violations.
- Where appropriate, designation of a compliance officer to oversee the implementation of the policy, procedures, and controls.
- Provision of related education and training to relevant personnel; and
- Independent reviews, monitoring and maintenance of the policy, procedures, and controls.

- The AML program of CAYC is designed to be compliant with:
- EU: “Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering”
- EU: “Regulation 2015/847 on information accompanying transfers of funds”
- EU: Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods
- BE: “Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash

3. Definitions

The following defined terms are widely used in the industry:

Money Laundering: The process of making illegally gained proceeds appear legal. This process is generally broken down into three steps: placement, layering and integration.

The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.

The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

The acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity.

Participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Placement: The process of placing unlawful proceeds into traditional financial institutions, through deposits or other avenues.

Layering: The process of separating proceeds of criminal activity from their origin using layers of complex financial transactions, such as converting cash into traveler's checks, money orders, wire transfers, letters of credit, stocks, bonds or purchasing assets.

Integration: Using apparently legitimate transactions to disguise the illicit proceeds, allowing the laundered funds to be distributed back to the criminal; integrating the now clean money back into normal use.

Suspicious Activity: Activity conducted by a user or non-user using the institution where there are indications that the persons engaging in the transaction may be doing so for fraudulent or illegal purposes.

Sanctions: Sanctions are activities conducted by the international community to prohibit or constrain activities of the target of the sanctions. For example, they are used:

- To encourage a change in behavior for a target country or regime.
- To apply pressure on a target country to comply with set objectives.
- As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed; or
- To prevent and suppress the financing of terrorists or terrorist acts.

4. Governance and Oversight

CAYC has appointed a Chief Compliance Officer ("**CCO**") that is responsible for coordinating the implementation of the AML Policy and policy program. The Chief Compliance Officer's duties also include developing AML initiatives, working with other Stakeholders to revise the AML policy, assessing new regulatory requirements and investigating potentially suspicious or unusual activity. CAYC also provides AML training to all its employees on a regular basis.

5. Know Your Customer and Transaction Monitoring

CAYC will apply appropriate user due diligence and ongoing monitoring measures required by law. CAYC will endeavor to prevent users from engaging in illicit or otherwise unauthorized activity. CAYC uses a combination of its software development and other service agreements, which are enforced through internal operational features to ensure that it complies with the applicable law.

Know Your Customer

A. Customer Due Diligence.

CAYC has adopted a risk based CDD to enable CAYC to understand the nature and purpose of the user relationship to the CAYC platform to develop a customer risk profile. To do so, CAYC collects certain documentary and non-documentary information at account-opening commensurate with the nature of the type of account and services that CAYC offers. CAYC maintains different CDD for different accounts and services.

For instance, the CDD requires users to go through CAYC's Identity Management System ("IMS"). The IMS consists of procedures for:

- Collecting baseline (e.g., wallet address, email address) information at account creation through CAYC's user onboarding portal.
- Monitoring the risk profile associated with the underlying cryptocurrency wallet used to fund the user's account.
- Maintaining records of the information used to identify the user; and
- Determining if a user appears on any list of known or suspected terrorists or terrorist organizations provided to the financial institutions based on the above information.

The above steps are operationalized using the following measures:

- **Identity and Age Verification.** A third-party service provider will support CAYC's ability to determine the legitimacy of the identification information other KYC materials or information provided and will confirm that the user is permissible. The service provider also will confirm that the user does not appear to be in a comprehensively sanctioned or otherwise prohibited jurisdiction and will search global sanctions lists to confirm that the user does not appear thereon using onboarding information such as wallet addresses.
- **Customer Information.** CAYC will collect details on each user to form a reasonable belief that CAYC knows the identity of its users commensurate with the user's risk profile. For instance, CAYC may collect such details as the wallet address, name, address, country, date of birth, or postal code (collectively, "KYC **Information"**). CAYC will collect any of the above KYC Information prior to issuing a CAYC funding address (e.g., QR code) to users. CAYC does not presently allow users who are non-natural persons. CAYC may, in its own description, rely on the performance by another institution of some or all the elements of our CIP.
- **Geo-blocking for Prohibited Jurisdictions.** CAYC will require contractual client certifications that, through IP address-based geo-blocking, no gaming services will be offered in countries where such activity is not permitted.
- **Geo-blocking for Sanctioned Jurisdictions.** CAYC also will require contractual client certifications that such users are not subject to United States, European Union, or other global sanctions or watch lists, including individuals or entities associated with the United States' comprehensively sanctioned jurisdictions, Iran, Cuba, North Korea, Syria, and the Crimean region of Ukraine. CAYC will rely on various risk-based measures to verify these representations including as in the below-described know-your-user ("KYC ") measures and through IP address-based geo-blocking.

- **Contractual Prohibitions on Users Onboarding from Prohibited Jurisdictions.** Users are notified at onboarding that CAYC does not offer services in restricted jurisdictions. CAYC's policy on restricting user activity stems from a combination of its risk, fraud prevention, and AML standards, as well as any assessments associated with the permissibility of its services in certain jurisdictions.

B. Enhanced Due Diligence and Ongoing Monitoring

CAYC performs ongoing monitoring on its users to detect any behaviors or indicators that might raise suspicions in regard to money laundering and terrorism financing practices. For that purpose, CAYC has implemented a set of red flag indicators that help it determine such behaviors and require further action from CAYC in assessing the customer information.

Whenever one of those red flags is triggered, the user account will be suspended and CAYC will pursue enhanced due diligence. Enhanced KYC diligence under this policy is deemed to include, but not limit to, the provision of:

- Full legal name.
- Country of citizenship.
- Permanent Address (which, for an individual, must be a residential or business street address, and for an entity, must be a principal place of business, local office, or other physical location).
- Identification number (either a taxpayer identification number, or, if unavailable, a passport number and country of issuance, alien identification card number or number and country of issuance of another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard).
- Identification Document; and
- Source of Funds and Source of Wealth.

CAYC may use third party service provider to verify any of the above information as determined to establish a reasonable basis to know the identity of the user where the user's activity warrants such action.

C. Acceptance Policy

CAYC will not accept a and will block the users that:

- Do not provide the identification information requested by CAYC.
- Provide fake identification documents.
- Try to use different means to deceive about their location.
- Are from restricted or prohibited jurisdictions; or
- Are subjected to United States, European Union, or other global sanctions or watch lists.

- Are gambling addicts or have mental health issues.
- Its source of funds originated or exchanges in restricted jurisdictions.

CAYC reserves the right to block and suspend players for any other reasons at its own discretion.

Transactions Monitoring

CAYC is firmly committed to complying with economic and trade sanctions programs imposed by jurisdictions in which the firm conducts business. For that purpose, CAYC established a transaction monitoring program with controls and processes to identify and detect any unusual activity in real time and in its ongoing monitoring.

CAYC will conduct ongoing monitoring on a regular basis using rule-based systems developed in-house and others from third-party vendors to review user history and patterns of activity to detect and report any unusual activity as required and to develop and implement any additional controls or limits in its platform.

CAYC implemented procedures addressing the following two key components of unusual or suspicious activity management:

- identification of unusual activity through methods of identification may include employee and customer identification, law enforcement inquiries, other referrals, or transaction and surveillance monitoring system reports; and
- alert management that focuses on processes used to investigate, evaluate and document identified unusual or potentially suspicious activity.

CAYC will use the following processes to achieve both goals:

- **Transaction Monitoring for Sanctioned or Prohibited Jurisdictions.** CAYC may in its reasonable discretion impose certain due diligence requests at user balance withdrawal. CAYC presently conducts a mixture of manual and automated transaction monitoring processes to identify "red flag" behavior. Where such red flag behavior is identified, CAYC may refuse to process any withdrawal attempts or collect additional information from the recipient. CAYC will further endeavor to limit any attempted user account funding from prohibited jurisdictions (which are identified in the CAYC user facing disclosures and updated from time to time internally) where the associated wallet address indicates that the user or the user's funds are in such a prohibited jurisdiction. For instance, CAYC may prohibit a user from funding their CAYC account using a known U.S. based exchange wallet as such assets indicate that the user is a U.S. person. Users will have the ability to rebut any suspension with additional information as part of CAYC's ongoing transaction monitoring and user due diligence standards.
- **Screening for Sanctioned Parties.** Prior to issuing a CAYC funding address to a user, CAYC may screen a user's wallet address against applicable sanctions databases. Such screening measures will rely on third party blockchain forensics vendors such as Chainalysis. CAYC will periodically re-screen wallet addresses against such databases.

- **Identification of Unusual Activity.** CAYC will monitor account activity for unusual size, volume, pattern, or type of transactions, considering risk factors and red flags that are appropriate to its business. Monitoring will be conducted running regular reports of unusual, high risk, or suspicious user activity.
- **Anti-Mixing Measures. CAYC** will utilize software designed to detect other suspicious deposit or withdrawal patterns. Such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk. In such instances, a user may be required to explain their methodology and purpose for using the platform.
- **Withdrawal Threshold KYC.** Additionally, and independently, every account, wherever or with whomever associated, will be suspended until adequate KYC diligence occurs once that account reaches a withdrawal threshold dependent on the accounts risk characterization over the life of the account.
-

D. Other Ongoing Monitoring Controls

Additionally, to the above-mentioned controlling procedures, CAYC has also implemented the following procedures to complement it know your customer and ongoing monitoring procedures:

- **Ban Evasion Detection.** In addition, CAYC will utilize third-party service provider software designed to detect the use by one user of multiple accounts. This software relies on detection of links between the same devices used to access multiple accounts. Such instances will be dealt with on a case-by-case basis, depending on the perceived level of risk. In such instances, a user may be required to explain their methodology and purpose for using the platform. CAYC accounts are funded by users using local (non-custodial) or hosted (custodial) wallets. CAYC monitors user activity within the CAYC platform, and any withdrawals must meet CAYC's and its third-party service provider's verification processes. CAYC further prohibits peer-to-peer account transfers within the CAYC platform infrastructure. Any attempts to circumvent this restriction will be treated as a red flag.
- **Time Zone Monitoring. CAYC** has implemented time zone controls that detect the user's device information and crosses it with restricted jurisdiction to understand if they are trying to use geo location software to hide the jurisdictions where they are connecting from.
- **Products and Services Review. CAYC** will establish additional procedures to avoid facilitating user attempts to exploit the CAYC platform. CAYC has a robust set of user-facing terms that users attest to utilize the CAYC platform. CAYC will establish certain additional safeguards to mitigate the risk of such misuse. For instance, CAYC may establish policies or procedures for limiting which user assets can be onboarded to the CAYC platform. CAYC lists the assets that are available for use on the CAYC platform. CAYC does not allow the use of anonymity enhancing technologies such as mixers, tumblers, or certain coins and tokens. Where CAYC becomes aware that an anonymity enhancing technology is being used on the CAYC platform, CAYC will disallow such use.

- **Vendor Management. CAYC** works with reputable third-party service providers as part of its compliance infrastructure. CAYC will periodically assess the strength of its key third party service providers to determine if additional services are needed, the third-party service provider is not performing consistent with its contractual obligations, or if other remedial action is necessary for CAYC to comply with this policy. CAYC may request information from any third-party service provider as part of its vendor review process.
- **Compliance Innovation.** In addition to vendor management, CAYC will continuously monitor any non-documentary compliance mechanisms to determine their viability for the CAYC program. CAYC may run tests or trial programs on a limited basis with such compliance vendors to determine the effectiveness of such programs. Blockchain native compliance tools include fraud prevention services, on-chain KYC providers, and other tools designed to reflect the technological features associated with blockchain platforms.

6. Education and Training

CAYC with the assistance of its legal counsel and under the oversight of its CCO, may provide employees AML, anti-terrorist financing and trade sanctions compliance training on a periodic basis, as deemed appropriate.

.

7. Reporting

CAYC is obliged to report any unusual or suspicious transactions, in accordance with the National Ordinance. Customers that are identified as being on a sanctions list, linked to money laundering or terrorism financing or other criminal activities will be reported as suspicious activity to the regulator.

8. Contact Details

The AMLRO of Eight Galaxies B.V.
Email: compliance@cayc.io

END OF DOCUMENT