Compliance Statement in regards to AstroBank' s Policies on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Policies.

Scope

AstroBank Public Company Limited (the 'Bank' or "AstroBank") in line and as required by the Laws, Regulations and Directives BY Competent Authorities, has established and implemented appropriate policies and procedures, that apply to the entire Bank, in order to achieve the timely and continued compliance of the Bank to the regulatory environment.

The goal is to ensure that the Bank is in compliance with the applicable legal and regulatory framework that governs preventing the use of the financial system for money laundering and terrorist financing and in this respect prevent the Bank from being used for any illegal activities and operations.

Legal and Regulatory Framework

The Bank is an Authorised Credit Institution supervised by the Central Bank of Cyprus ('CBC'). The CBC is the competent authority for the enforcement of the provisions of the legislation in relation to the financial activities of supervised entities in Cyprus, under section 59(1)(a) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2019 ('the AML/CFT Law'). Under the Law the CBC has issued the 5th edition of the Directive on the Prevention of Money Laundering and Terrorist Financing ('the CBC AML/CFT Directive').

In 2020, the CBC also issued the first Directive for Compliance with the Provisions of UN Security Council Resolutions and the Decisions/Regulations of the Council of the European Union.

Moreover, the CBC regularly issues various guidelines and circulars on key areas of concern, such as customer identification procedures and due diligence measures, the ongoing monitoring of accounts and transactions, record keeping, internal reporting mechanisms, trainings, politically exposed persons, tax issues and other risk management measures.

The above constitute the main legal and regulatory framework within which the Bank is obligated to operate. The Bank has specific procedures and mechanisms in place, which have been designed to implement the "Know your Customer" and the "Know Your Transaction" principles as well as the Customer Due Diligence (CDD) concept. These, form the core part of the Bank's Anti-Money Laundering policy.

For the monitoring and assessing of any potential AML/CFT risks and the drafting of internal manuals, policies/procedures the Bank also reviews and considers the guidelines, recommendations and opinions of International and European bodies such as the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the Financial Action Task Force (FATF).

In regards to sanction regimes, AstroBank fully adheres to the the United Nations Security Council resolutions, the EU, the Office of Foreign Assets Control of the U.S. Treasury

Department and the UK Office of Financial Sanctions Implementation. In addition, G7 sanctions are used as need for EDD. These sanctions are closely monitored as an additional control to the effectiveness of the automatic update of the relevant AML systems.

Customer Acceptance Policy

The Bank, in line with the Directive of the Central Bank of Cyprus has issued the Customer Acceptance Policy and relevant procedures, which outline the categories of:

1) customers with whom a business relationship with the Bank is prohibited,
2) high risk customers for whom enhanced due diligence and monitoring is required.

1) Customers with whom a business relationship with the Bank is prohibited

The following services and types of customers are considered as extremely high risk and are not accepted by the Bank:

- Customers for which the activity appears to relate to any form of illegal activity including without limitation bribery, fraud, money laundering, terrorism financing, human trafficking, political corruption, illegal wildlife trafficking, tax evasion, prostitution, child pornography, slavery, drug dealing.

- Customers that appear to have illegitimate purpose for registering a company, for example, a customer is registered company in a tax heaven jurisdiction for the purpose of receiving commission which is the result of conflict of interest or corruption.

- Customers involved in arms, munitions and equipment of dual use that intent to be used for military purposes.

  Excluded from this are Cypriot based importers of guns and equipment that are permitted and licensed by the Republic of Cyprus. The purpose of which is to be used within the Republic for hunting and recreational purposes.

- Unregulated casinos and/or online casinos and/or unregulated gambling.

- Customers involved in internet gambling that is either unlawful or not licensed by the Republic of Cyprus. The prohibition includes entities and / or individuals who offer services (e.g. payment providers, software houses, card acquirers) to the persons involved in non-Cypriot or non-EU regulated electronic gambling through the internet.

- Unregulated exchange bureau,

- Clients with either anonymous, or secret accounts; or accounts in fictitious names or numbered accounts. All accounts shall open in the name as appears on the official identification documents.

- Shell banks. The Bank's policy prohibits entering into any relationship with as it appears a shell bank. Furthermore, it is required that appropriate measures are taken to

ensure that the Bank does not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

- Trusts and government bodies which originate from countries subject to financial sanctions which are issued by the United Nations ("UN"), the European Union (EU) or any member state, the Office of Foreign Assets Control ("OFAC") including all of its subcategories, and United Kingdom (UK).

- Individuals or entities subject to / or related to the restrictive measures issued by any of the above-mentioned Authorities and/or customers that transact or associate with sanctioned individuals and/or legal entities.

- Customers with operations that may violate export controls or circumvent capital controls imposed by governments and/or Central Banks.

- Charitable Trusts and Foundations or Discretionary Trusts with no declared Beneficiaries. Excluded are Trust and Foundations that have a proven record and substance as charitable organization.

- Customers who do not provide sufficient identification evidence or disclose their financial operations. The Bank's policy requires that in the event that it cannot comply with the customer identification and due diligence requirements set out in the Law and the CBC Directive, it should not:
    a. execute a transaction through a bank account,
    b. establish a business relationship or
    c. execute a once-off transaction.

  Existing relationships, should be terminated and consider whether it is warranted, under the circumstances, the Bank employee to submit an ISR directly to the AMLCO.

- Customers who provide financial or insurance services without a license or authorization by a competent supervisory/regulatory authority of an EU country or a third country of equal AML standards and legislation.

- Payable through accounts.

- Walk-in persons requesting funds to be transferred to non-customers.

- Individuals or entities operating in adult entertainment services. This includes holding companies who operate such operations throughout subsidiaries and / or affiliates. The prohibition also relates to companies that provide the software / platforms for such websites that belong to the same group of companies, or companies that are directly, or indirectly, involved in such services.

- Customers involved directly or indirectly with virtual currencies, as Virtual Asset Service Providers (VASPs) including virtual currency exchanges, administrators.

- Shell companies, as defined by the CBC AML/ CFT Directive.

- Companies with shares that are issued on the bearer except when such companies are part of a well-known group and in this case are marked as HR as described below.

- Accounts in the name of non-EU regulated corporate service providers or Client Accounts for ASPs regulated by CySEC excluding for Approved Introducers of AstroBank in which case are HR customers.

2) <u>High risk customers for whom enhanced due diligence and monitoring is required</u>

Customers who may pose a particular risk to the reputation of the Bank and should normally be treated as high risk and are subjected to enhanced Customer Due Diligence, include, but are not limited to the following:

- Customers falling within the definition of Politically Exposed Persons (PEPs) including local PEPs;
- Private Banking customers offered investment services as foowing categories:
    - Non-EU Individuals
    - Cypriot registered companies with non-EU UBOS
    - Non-cypriot registered companies regardless of the residency of the UBOs.
- Customers from countries which inadequately apply the FATF recommendations.
- Companies whose shares are in the form of bearer;
- Trusts and foundations;
- Companies in the names of third parties (i.e. client accounts) ;
- Escrow Accounts;
- Customers involved in gambling / gaming industry / casino management companies licensed by the Competent Authority of the Republic of Cyprus
- Customers which have been rejected by other banking institutions or customers for which negative information was identified;
- Accounts belonging to Unions, Clubs, non-Cypriot Provident Funds and charitable organizations;
- Customers that form part of complicated/complex corporate structures;
- Customers vulnerable to tax evasion;
- Customers whose line of business relate to precious stones and metals, oil and related items, tobacco and alcohol.
- Funds
- Customers categorised high risk as per AMLCO decision

Appropriate controls are in place to manage the risks posed by the above, either automatically or manually. All high risk customers are approved by Senior Management after having received the opinion of the Compliance Unit. Furthermore, all high risk customers are reviewed on an annual basis in relation to KYC documentation and transactional behavior.

All Units with high risk business ensure close monitoring of transactions to ensure that any unusual and potentially suspicious activity is duly and promptly identified. In this respect, an automated anti-money laundering system has been outsourced for account monitoring purposes via the production of Anti-Money Laundering and Watch List Management alerts.

Know Your Customer Principle (the "KYC")

The Bank places special emphasis on the KYC principle and there are specific procedures in place for its implementation based on a risk-based approach depending on the risk level of customer. Satisfactory KYC information is always obtained prior to commencing a business relationship and should be updated on a regular basis during the course of the relationship.

Sanctions Compliance Policy

Pursuant to the circulation of Directive for Compliance with the Provisions of the UN Security Council Resolutions and the Decisions and Regulations of the Council of the European Union of 2019 (First edition) that was published by the Central Bank of Cyprus in March 2020, the Bank has designed a Sanctions' Compliance Policy setting out the main obligations of the Bank that arise from the provisions set therein.

Apart from the obligations deriving from the Provisions of Central Bank of Cyprus' Sanctions' Directive, the Bank also complies with the economic sanctions and trade embargoes issued by the Office of Foreign Assets Control (OFAC) and the UK Office of Financial Sanctions Implementation made under the Sanctions and Anti-Money Laundering Act 2018.

Training

The Bank has in place adequate and appropriate systems and specific procedures for the ongoing education and training of staff with regards to the relevant local and EU law and directives on the prevention of money laundering and terrorist financing and sanctions. Special attention is given to the training of the Bank's staff in order to recognize and handle transactions and activities suspected of being related to money laundering and terrorist financing. Sanctions related training also takes place in accordance with the current sanctions' developments and sanctions evasion techniques.

Correspondent Banking

The Bank has in place specific procedures for the establishment of correspondent banking relations with other financial institutions in compliance with the Wolfsberg principles, the Patriot Act, FATCA, Common Reporting Standard, the Law, the Directive and Guidelines.

Money Laundering Compliance Officer

A senior official of the Bank has been appointed as the Money Laundering Compliance Officer, ('MLCO') who reports to the CEO of the Bank for administrative purposes and directly to the Audit Committee of the Board of Directors of the Bank through the presentation of the quarterly Risk Assessment Reports.

The MLCO is responsible for the implementation, coordination and oversight of the Bank's Anti-Money Laundering Policy. More specifically any transaction and/or activities which are believed to be suspicious are reported to the MLCO where the suspicions will be further investigated. In cases where it appears, or it is strongly suspected, that an account is being used for criminal purposes, it is reported to the relevant authorities / local FIU.

The MLCO is also responsible for the submission of the following reports to the Senior Management of the Bank and the Central Bank of Cyprus:

- Annual Report and Risk Assessment Report submitted to the Board of Directors through the Senior Management for their consideration and approval. A copy of the said reports is also submitted to the Central Bank of Cyprus.
- Quarterly Risk Assessment Report submitted to the Audit Committee of the Board of Directors of the Bank.

Risk Assessment Program

The Bank's risk assessment program takes into account the Bank's customers, specific products and services that are offered to customers, channels of distribution of the products /services and countries with which the customers or intermediaries are connected.

Operational Controls - Co-operation with the Authorities

It is the Bank's policy and practice to fully co-operate with any official authorities related to money laundering always within the framework of the law.

Operational Controls – Record Keeping

The Bank keeps appropriate records, in relation to transactional and customer identification data, for a period of at least 5 years (some types of documents are never destroyed) after the termination of the relationship, plus 5 years more for cases related to Compliance.

Operational Controls - Screening of Customers and Transactions

All customers of the Bank are screened against, among others, United Nations, European Union, OFAC and UK sanctions lists as well as the World-Check database prior to the commencement of a business relationship, to ensure that the Bank complies with applicable sanctions regimes and that no customer is accepted and no transaction is executed which falls outside the Bank's policy. The Bank is also in a position to perform additional checks, when deemed necessary, through the LexisNexis database.

The Bank has in place automated systems for the purpose of verifying, prior to the execution of any transaction, that no counterparty is in violation of any sanctions regime or is on any list of known or suspected terrorists issued by the UN, EU, OFAC and UK and other competent authorities. In addition to the foregoing controls, the Bank has in place an automated system for screening transactions aiming at identifying any unusual and suspicious transactions behavior.

Reliance on third parties (Introducers)

The Law permits the Bank to rely on third parties for the implementation of customer identification and due diligence procedures. The Bank has a comprehensive process in place for the assessment of the prospective introducers as well as a review process for the ongoing evaluation of the existing third parties. The procedures are designed in order to minimize the risks associated with Introducers.

Independent Audits

The Internal Audit Unit of the Bank as well as the External Auditors perform annual audits of the Compliance Unit.

AML findings identified during audits of other units of the Bank by the Internal Audit Unit are communicated to the Compliance Unit for evaluation and for appropriate action where needed.

AstroBank Public Company Limited
Compliance Unit
January 2024