STATEMENT OF ANTI-MONEY LAUNDERING (AML) AND COUNTER-TERRORIST FINANCING (CTF) POLICIES AND PRINCIPLES

Scope

AstroBank Limited (the 'Bank') 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 with the current anti-money laundering ('AML') and combating the financing of terrorism ('CFT') regulatory framework.

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 operations.

Framework

In 1996, the Republic of Cyprus enacted the Prevention and Suppression of Money Laundering Activities Law (the 'Law') which designates the Central Bank of Cyprus as the competent supervisory authority for all banks operating in Cyprus and assigns to it the responsibility of ensuring banks' compliance with the provisions of the Law.

Under the said Law, the Central Bank of Cyprus has issued the 'Directive and Guidelines on the Prevention and Suppression of Money Laundering and Terrorist Financing' (the 'Directive' and the 'Guidelines') which requires banks to implement customer identification, transaction monitoring, record keeping, internal reporting, training and other procedures for the prevention of money laundering.

The current Law, 'The Prevention and Suppression of Money Laundering Activities Law 2007-2013', which in effect amended and consolidated the previous Laws, harmonised the Cyprus legislation in accordance with the Third European Union Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Directive 2005/60/EC) and is in line with the Recommendations of the Financial Action Task Force ('FATF'). The Bank has specific procedures designed to implement the "Know your Customer", "Know Your Transaction" principles and the due diligence concept which form the core part of the Bank's Anti-Money Laundering policy.

Customer Acceptance Policy

The Bank, in line with the Directive of the Central Bank of Cyprus 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:

- Arms dealers;
- Unregulated casinos and exchange bureaux;
- Anonymous accounts, accounts in fictitious names, numbered accounts;
- Shell Banks;
- Individuals or entities known or suspected to be a terrorist or a criminal organisation;
- Trusts and government bodies which originate from countries subject to financial sanctions which are issued by the United Nations or the European Union;
- Individuals or entities subject to the restrictive measures issued by Office of Foreign Assets Control ('OFAC'), or in accordance with relevant regulations of the European Union and United Nations Security Council Resolutions;
- Persons involved in electronic gambling / gaming through the internet without a license issued by the Republic of Cyprus. The prohibition also extends to individuals or entities who offer services (e.g. payment providers, software houses, card acquirers) to such persons;
- Customers who do not provide sufficient identification evidence;
- Customers who provide financial or insurance services without license or authorization by the competent supervisory/regulatory authority;
- Payable-through accounts;
- Walk-in customers for whom there is insufficient identification evidence as well as funds transfers for non-customers;
- Individuals or entities operating in adult entertainment network services;
- Any transactions involving certain countries subject to embargo.

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;
- Customers from countries which inadequately apply the FATF recommendations;
- Non-face-to-face customers;
- Companies whose shares are in the form of bearer;
- Trusts/foundations;
- Companies in the names of third parties (i.e. client accounts) ;
- Escrow Accounts;
- Customers which have been rejected by other banking institutions;
- Correspondent banking customers from non-EU countries;
- Customers involved in gambling/gaming industry licensed by the Republic of Cyprus;
- Accounts belonging to Unions, Clubs, Provident Funds and charitable organizations;
- Customers for which the completion of a questionnaire regarding the customer's activities was requested by a correspondent bank;
- 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.

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.

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,. 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.

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.

Operational Controls - Screening of Customers and Transactions

All customers of the Bank are screened against, among others, United Nations, European Union, OFAC 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 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 as well.

AstroBank Limited
Compliance Unit
31 March 2017