

## **LAIKI GROUP ANTI-MONEY LAUNDERING STATEMENT**

In 1996, Cyprus enacted the Prevention and Suppression of Money Laundering Activities Law (hereinafter to be referred to as the “Law”) which contains both suppressive and preventive provisions against money laundering. Since its enactment the Law has been subject to several amendments in order to give effect to a number of new international initiatives and standards in the anti-money laundering field. The Law is in full conformity with the European Union’s Directives on the prevention of the use of the financial system for the purpose of money laundering (Directive 91/308/EEC as amended by Directive 2001/97/EC), the Council of Europe’s 1990 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the Financial Action Task Force’s (“FATF”) revised 40 Recommendations.

Cyprus’s anti-money laundering legislation criminalises money laundering from all crimes punishable with imprisonment in excess of one year and requires all credit institutions, investment firms, insurance companies as well as lawyers (in respect of financial business) and accountants, real estate agents and dealers in precious metals and stones to implement strict procedures for preventing the use of their services for money laundering. In this regard, persons subject to the Law are required to implement procedures for customer identification, record keeping and internal reporting as well as to ensure that their employees are aware of their obligations under the Law and receive adequate training designed to assist them in recognising money laundering transactions. They are also required to appoint properly qualified persons as “Money Laundering Compliance Officers”.

The Law 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’ due compliance with the provisions of the Law.

Under the said Law, the Central Bank of Cyprus has issued several Guidance Notes which require banks to implement customer identification, record keeping and other procedures for the prevention of money laundering, including the identification of beneficial owners of accounts and transactions and checks on the source and legitimacy of funds flowing through the banking system in Cyprus.

The most important legislative development in 2004, has been the reissue of the revised Guidance Note of the Central Bank of Cyprus concerning the Prevention of Money Laundering which takes account of the following:

- The amendment of the prevention and Suppression of Money Laundering Activities Law (Law 61(I) of 1996) of July 2003, for the purpose of harmonizing Cyprus’s legislation with the Second EU Money Laundering Directive of December 2001.
- The revised 40 Recommendations for combating money laundering issued by the Financial Action task Force (FATF) on money laundering in June 2003.
- The FATF’s 8 Special Recommendations on terrorist financing issued in October 2001.
- The Basel Committee on Banking Supervision’s paper on “Customer due diligence for banks” issued in October 2001.

The major changes relate to the:

A. Development of customer acceptance policy

Banks should develop clear customer acceptance policies and procedures, which should provide for enhanced due diligence procedures for high risk customers. These policies and procedures should take into account factors such as the customers' background, country of origin, anticipated level and nature of the business activities as well as the expected origin of the funds.

B. Renewal of customer identification

Banks need to undertake on a regular basis or wherever there are doubts about the veracity of the identification data, reviews of existing customer identification data especially for high risk customers. If the bank becomes aware that it lacks sufficient information about an existing customer it should take all necessary action to obtain such information as soon as possible.

C. Prohibition of secret, anonymous, numbered accounts as well as accounts in fictitious names

D. Construction of customers' business profile

In addition to the necessary measures that the banks should undertake for the establishment of the beneficial owners of the accounts at the outset of the business relationship they should also obtain sufficient information with the aim of constructing customers' business activities and expected pattern of transactions, which as a minimum should include:

- The purpose and reason for opening the account or requesting the provision of services;
- The anticipated level and nature of the activity to be undertaken;
- The anticipated account turnover, the expected origin of the funds to be credited in the account and expected destination of outgoing payments; and
- The customer's source of wealth or income, size and nature of business/professional activities.

E. Installation of appropriate computerised systems for the purpose of verifying as to whether a customer constitutes a "Politically Exposed Person".

F. Assessment of customer identification and due diligence procedures employed by professional intermediaries and third party introducers for the purpose of accepting customer identification performed by the said persons when they introduce customers to the banks as well as the conclusion of an agreement under which it is permitted to the bank at any stage to verify such due diligence procedures.

G. Provisions of full details on the ordering in all messages for funds transfers in excess of US \$1.000 performed by electronic means.

H. Introduction and implementation of adequate management information systems for the purpose of on-going monitoring of customers accounts and transactions.

Furthermore, the Central Bank of Cyprus is applying a very strict supervisory regime over banks which entails, besides the issue of Guidance Notes for the implementation of preventive measures, off-site and on-site inspections which aim at assessing banks' compliance with their anti-money laundering obligations.

The major challenge facing the banking system today is the requirement set by the Central Bank of Cyprus that all banks are obliged to put into operation adequate management information systems for the on-going monitoring of accounts and transactions within a specified period of time. All major money laundering issues are discussed at regular intervals at the Cyprus Association of Commercial Banks.

A prospective customer's identity should be obtained and verified using reliable, independent documentary and / or electronic source material. Where such evidence is not provided then the business should be declined. Where there are doubts about the quality or adequacy of previously obtained customer identification material for existing customers then, on the basis of materiality and risk, identification / verification should be carried out at appropriate times (e.g. immediately for high risk customers; when a transaction of significance takes place; when there is a material change in the way in which the account is operated; etc).

In no circumstances may accounts be operated or relationships established for anonymous customers or in obviously fictitious names or for a shell bank as defined by the Financial Action task Force (FATF).

For non-personal customers (e.g companies (particularly private companies), trusts, partnerships, etc) measures should be undertaken to understand the ownership and control structure (including the person/s who is / are able to exercise control over the funds), and appropriate identification and verification undertaken.

Special care is taken in respect of customers introduced by intermediaries, particularly where use is made of shell companies (companies which do not have a physical presence in their country of incorporation), trusts, nominee structures or other structures which appear to be established in order to hide the true ownership of assets. In all such circumstances the details of the identity and supporting identification material in respect of all relevant parties must be obtained and verified. The acceptance of business introduced by or managed through any intermediary is subject to appropriate and satisfactory initial and ongoing due diligence in respect of the intermediary. Approved relationships with intermediaries should be reviewed and re-approved on a regular basis.

KYC information is generally obtained prior to commencing the relationship and should be updated on a regular basis during the course of the business relationship. A risk-based approach should be applied depending on the type of customer, nature of the business relationship, product and any other risk factor that may be relevant. Customer file records are kept forever.

KYC information includes but is not limited to:-

- Appropriate personal, business and financial details with regard to the customer.
- Details on the purpose and intended nature of the business relationship including anticipated transactional activity.
- Details as to the source of funds/wealth.

Regular monitoring is undertaken by line management and/or Compliance to check that all businesses comply with the Group's AML Policy and Principles, standards and procedures as well as legal and regulatory requirements. The Audit Committee of the Board of Directors is briefed regularly on new developments or other issues arising.

Group Compliance is assessed periodically both by Group Internal Audit as well as by the bank's external auditors.

All new staff who may be involved in customer business must receive introductory training to ensure that they understand the AML Group Policy and Principles. The Prevention and Suppression of Money Laundering Activities Law, enacted in 1996, requires Banks to establish a programme for continuous staff training. In compliance with the Law, Laiki Bank organises a series of training seminars throughout the year for all bank employees all over Cyprus. The training program of staff includes training at regular intervals and at different levels of authority and expertise, that is, induction courses, courses for tellers, for account managers etc. In addition, a number of specialised anti-money laundering training sessions are organised every year, for example, for the Private Banking and the International Business Units.

The risk assessment program is based on the country of origin, the type of customer, the nature of customer's business, as well as on the type of product offered. Under normal circumstances an updating of the customers and associated transactional risk is carried out on an annual basis. The bank's policy prohibits business with arm dealers, non-regulated casinos and other high risk segments.

Our Correspondent Banking Department has in place internal standards for the establishment of correspondent relations with financial institutions based on the Wolfsberg principles and the Central Bank of Cyprus's Guidance Notes. They differ from country to country according to the regulatory and legal framework, the size and structure of the financial institution and include an assessment of the correspondent's Anti-Money Laundering Policy.

All Units with high risk business ensure appropriate scrutiny and monitoring of transactions, account activity and customers are undertaken in order to identify unusual and potentially suspicious activity.

The Group has developed a number of AML exception reports to support these controls which, are undertaken at different levels, whilst an automated transaction monitoring system is under development.

Every Business Unit in the Group must have procedures in place so that any transactions and/or activities which are believed to be suspicious are reported to the Money Laundering Compliance Officer where the suspicions will be validated.

Where the Group or an employee is put on notice that a particular customer or a particular type of transaction should be treated with caution, then it may be necessary to review the accounts or transactions in question. For example:

- When a transaction for a customer is identified as being suspicious, other transactions for that customer should be reviewed;
- When a customer's activities on one account have been identified as suspicious the customer's other accounts and any connected accounts should be examined;
- Where suspicions are aroused on an account managed by an agent or introduced by an intermediary or in other similar circumstances, any other accounts managed by that agent, introduced by that intermediary etc. should be reviewed;

In cases where it appears, or it is strongly suspected, that an account is being used for criminal purposes, it should usually be closed, subject to any views by the authorities and to any legal or regulatory constraints.

All suspicious transactions reported by the branches / units are investigated by Group Compliance and if the suspicion is valid a Suspicious Report is sent to the unit for Combating Money Laundering (MOKAS).

For further information or enquiries please contact Group Compliance, LAIKI GROUP.