Procedures for Prevention of Money Laundering & Know Your Client

May 16 2017

Objectives

To implement control and communication systems to prevent the company from being used for money laundering.

Establish customer acceptance policies and procedures.

The implementation of the objectives is based on the following points:

1. The appointment of the Chief Financial Officer, Darlene Hart, as responsible for the supervision and compliance with these regulations and standards. The CFO has sufficient experience, seniority and independence to carry out this position;
2. Establish and maintain procedures for the identification, verification and origin of customer funds (KYC), including due diligence for those clients who are at greater risk, such as politically exposed persons (PEPs);
3. Establish and maintain systems and procedures to monitor the client activity ;
4. Establish procedures for the reporting of suspicious activity internally and to the competent authorities, as appropriate;
5. The maintenance of appropriate records;
6. Training of all relevant employees.

Know Your Client

The initial and most vulnerable phase of money laundering is placement. The aim is to introduce illegal income into the financial system without attracting the attention of financial institutions or law enforcement authorities.

Placement techniques include the splitting of currency deposits into sums that evade reporting requirements or the combination of legal and illegal currency deposits. An example may include: dividing large sums of cash into smaller, less conspicuous sums, which are deposited directly into a bank account; deposit a check received as a refund for the cancellation of a vacation package or insurance policy; or purchase a series of monetary instruments (eg, cashier's checks or money orders) that are then collected and deposited in accounts of other localities or financial institutions.

Segmentation by client’s risk

The risks inherent in monitoring money laundering or terrorist financing can be more effectively undertaken if the potential risk is linked to different types of customers and their operations. Orocrypt customers will be identified by risk levels, in order to design and implement measures and controls to mitigate such risks, as well as to exercise greater control over clients and transactions that present greater risk. Likewise, once the relationship with the client has been formalized, a continuous follow-up of the same and the operations carried out by the client will be monitored.

Registration

Each investor will need to register and provide certain information to us. **We cannot sell to US persons.**

a. Investments of less than 5 thousand euros: Name, address, email , telephone. Prior to receiving the tokens, the clients must send proof of identification by uploading a scan or photograph. Acceptable documents are passport, national registration document or driving license.

b. Investments between 5 to 50 thousand euros: Same as above plus a scanned high resolution photograph of the investor holding his/her passport and a scanned copy of a utility invoice or bank statement showing the investor’s address.

c. Investments over 50 thousand euros: Same as b. above plus a statement regarding the source of funds, eg. from beneficial owner's accounts or from a third party, sale of property/assets, investment loan, etc., and a bank letter of reference.

Customer identification and knowledge

The obligation to identify and know the client and his activities is established as a due diligence measure. This obligation will be fulfilled according to the risk present in the business, activities and countries in which it is operated and related to the operations that are carried out.

To this end, the following guidelines will be followed:

- Know and document the true identity of customers who maintain any type of commercial relationship through proper documentation and / or processes.
- Know and document any additional information about the client, in accordance with the assessment of the risks of money laundering and terrorist financing.
- Refrain from carrying out operations with individuals or entities whose identities are not confirmed, or who do not provide necessary information or have provided false information.
- Do not open or maintain anonymous accounts or accounts with fictitious names.
- To know the identity and to accredit the power of representation of the people who authorize financial transactions on behalf of clients.
- Obtain information on the true identity of the person on whose behalf an account is opened, or an operation which is carried out when the client acts on behalf of third parties or in cases where there is doubt as to whether the client acts on his/her own behalf.
- In the case of legal entities, except those listed in a regulated market, identify any natural person who ultimately owns or controls, directly or indirectly, 25% or more of the shares rights or assets.

At the time of establishing a relationship or opening an account, according to the valuation of risk, the following additional guidelines should be followed:

- Determine the origin of the client's funds.
- Confirm the information provided by the client.

Clients banned or with reinforced acceptance measures

In order to control the risk of money laundering and the financing of terrorism, Orocrypt Inc. will not accept clients from whom the necessary data is not available or who fall into one of the categories detailed below and in the effects of this framework and its developments, will be considered forbidden clients:

- Persons included in any of the official lists of sanctions, involving a connection with a prohibited country, with persons (physical and legal) resident or incorporated in a prohibited country or related to the government or official state institutions (even if they reside outside the forbidden country).
- Persons over whom information is available from which it may be inferred that they may be related to criminal activities of money laundering or terrorist financing, and underlying crimes.
- Persons who refuse to provide information or required documentation.
- Legal persons whose shareholding structure or control can not be determined.

For PEPs, the application will be reviewed and approved by the Board.
Politically exposed people and their families and relatives. (PEPs). PEPs are defined as individuals who fulfil or have been entrusted with prominent public functions, such as heads of state or government, senior politicians, senior government or judicial officials, or senior military personnel, high-level executives of state-owned companies and important political party officials. Family and close relationships are defined as the spouse or person permanently linked by a similar relationship of affection as well as parents and children, and the spouses or persons linked to the children.

Analysis and operational control

Continuous monitoring of the business relationship with all types of customers, in order to detect suspicious transactions, must be established. In order to do this, the type of operations, business sector, geographical area and transactional volume will be regularly monitored.

The monitoring of clients and high-risk operations should be more intense and should take into consideration key indicators for these clients and their accounts, considering circumstances such as country of origin, the source of their funds, the type of transactions and other risk factors.

Communication of suspicious transactions to the authorities and communication

Orocrypt Inc. will perform the required reporting duties and will collaborate with the competent authorities. The employees will immediately report the suspicious transactions to Director Darlene Hart responsible for this area, so that she, in accordance with the law, makes the necessary checks and the appropriate reports or communications of suspicious operations to the authorities when it is considered that:

- May be related to funds from criminal activities or hide funds or assets originated by these activities.
- Can commit funds that are directly or indirectly used, in whole or in part, for the commission of activities of a terrorist nature.
- They are divided or structured to circumvent some of the records or systematic communications.
- They have no commercial purpose or there is no reasonable explanation for such operations.

When the units or employees make communications about suspicious operations or activities to Director Hart, following the procedure established in the internal regulations, it will be totally prohibited to provide any information, both internal and external, on the clients or operations to which the information refers . In the same way, compliance with both the legislation and the internal regulations on blocking transactions and capital movements and / or prohibiting the opening of accounts regarding natural or legal persons on which such measures have been issued will be ensured.

Conservation and archiving of documents

The necessary documents listed below will be kept for a period of at least three years, or longer if applicable to local regulations (according to each jurisdiction):

- The documentation that contains information on the identification and knowledge of the clients.
- Reports submitted to the authorities on suspicious activity of a client relating to a possible case of money laundering and / or terrorist financing, together with the documentation that supports them.
- The records of all courses on the prevention of money laundering and the financing of terrorism that have been given.
- Any other documents or records that need to be kept under the laws against money laundering or the financing of terrorism.
- The said documentation or information will be properly archived on durable media, so that its location is facilitated and its confidentiality guaranteed.

Training for the prevention of money laundering and terrorist financing

All staff should receive ongoing training on the requirements of the regulations on the prevention of money laundering and the financing of terrorism. To do this, the following guidelines or principles should be followed:

- Existence of training plans and special courses that, addressed to their managers and employees and specifically the personnel who perform those jobs that, because of their characteristics, are suitable for detecting the facts or operations that may be related to money laundering or terrorist financing.
- Training plans and programs must identify the staff in need of training.
- It is necessary to register all the formative action imparted, leaving record of its main characteristics and elements.
- Irrespective of the general training plans, all persons responsible for money laundering must be informed and permanently inform the dependent employees of any changes in regulations in this area, as well as all new modalities, techniques or procedures that are detected as being likely to be used for money laundering or the financing of terrorism.