ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

To : **Regulated Entities**
- **i. Cyprus Investment Firms ('CIFs')**
- **ii. Administrative Service Providers ('ASPs')**
- **iii. Undertakings for Collective Investment in Transferable Securities ('UCITS')**
- **iv. UCITS Management Companies ('UCITS MC')**
- **v. Alternative Investment Fund Managers ('AIFMs')**
- **vi. Alternative Investment Funds ('AIFs')**
- **vii. Alternative Investment Funds with a Limited Number of Persons ('AIFLNPs')**

From : **Cyprus Securities and Exchange Commission**

Date : **23 February 2018**

Circular No : **C260**

Subject : **Common and recurring weaknesses and/or deficiencies and best practice standards identified during the onsite inspections performed in relation to the prevention of money laundering and terrorist financing**

The Cyprus Securities and Exchange Commission ('the CySEC') wishes to inform the regulated entities of the following:

During the year 2016-17, the CySEC performed onsite inspections of the entities under its supervision ("regulated entities") to assess their compliance with the Prevention and Suppression of Money Laundering and Terrorist Financing Law ("the Law") and the Directive DI144-2007-08 on the Prevention of Money Laundering and Terrorist Financing ('the Directive').

The results of the onsite inspections found a significant improvement in the internal procedures and measures applied by regulated entities to prevent money laundering and terrorist financing, in compliance with the Law and Directive.

While CySEC has identified some best practice standards applied by regulated entities, it has also identified common and recurring weaknesses and/or deficiencies which CySEC, in addition to the measures already taken to ensure full compliance, calls upon all regulated entities to duly consider and immediately implement corrective measures.

A. Best practice standards

When carrying out its onsite inspections, CySEC has identified the following best practice standards. These best practice standards are outlined to serve as a reminder of how regulated entities must uphold their duty to maintain and improve the systems, controls and procedures for the prevention of money laundering and terrorist financing:

- Introduce and adopt policies for not accepting cash as a form of payment.
- Return deposited funds to customers by way of the same bank account from which they originated, always in the same name of the customer.
- Apply automated electronic systems for:
  - Identifying customers and conducting ongoing customer due diligence. This includes the verifying and updating of the data and information collected;
  - Monitoring customer transactions to detect and investigate those that fall outside the normal and reasonable account activity of the customer. Transactions should also be monitored for unusual or suspicious transactional behaviour that is inconsistent with the economic profile of the customer, including those transactions without obvious economic or legitimate purpose.
- Employ specified staff members charged exclusively with the duty and responsibility of implementing practices, measures, procedures and controls related to the prevention of money laundering and terrorist financing.
- Increase the education and training provided to all staff, including board members, to improve and maintain their knowledge of anti-money laundering and counter financing of terrorism processes and controls.
- Take immediate corrective action to address any weaknesses and/or deficiencies identified by CySEC during onsite inspections.

B. Common and recurring weaknesses and/or deficiencies

CySEC identified these common and recurring weaknesses and/or deficiencies in regulated entities compliance with the Law and Directive when carrying out its onsite inspections.

i. Customer Due Diligence

- A risk-based approach to verifying the collected customer or beneficial owners' data and information should be taken. CySEC found weaknesses in these processes, contributing to poor customer economic profile-building. This included insufficient measures taken to verify sources of customer wealth and funds.
- Processes of obtaining and assessing information about customers or beneficial owners' backgrounds were also deficient**.** This meant that regulated entities were not fully equipped to conduct accurate identification, recording and evaluation of the risk posed by customers.
- Policies establishing and delivering to timeframes set to ensure information and data collected on customers is kept up to date must be followed. These timeframes are based on

the customer's risk categorisation, but should be flexible to encompass any event or incident that is provided in the Law and/or Directive or that may change a customer's risk categorisation. In addition, a separate form (printed or electronic) containing customer data should be also regularly maintained with up-to-date information.

- Lastly, CySEC found areas of weaknesses in the application of enhanced due diligence measures. This included high-risk customers, especially true of dealings with **non-face-to-face customers**.

ii. Timing of verification of the customers' identification

- On some occasions, when regulated entities use the exception to the rule of verification of customer identity and beneficial owner before the establishment of the business relationship, the verification of the identity of the customer and beneficial owner is completed **during** the establishment of the business relationship. In these instances, CySEC has noted that the requirements of Circular C157 are not always fully met. The requirements include a maximum amount of deposited funds limited at €2,000 and a maximum 15-day timeframe to complete the customer's identity verification process. If this is not verified within 15 days, the regulated entity is obliged to terminate the business relationship and return deposited funds to the customer to the bank account of origin immediately.

iii. Termination of the business relationship with customers

- On some occasions, regulated entities failed to record in their risk management and procedures manual, the circumstances of terminating a business relationship with their customers. This includes the failure or refusal by customers to submit, within a reasonable timeframe, the required data and information for the verification of their identity and the creation or update of their economic profile.
- In some instances, regulated entities **failed to terminate the business relationship** with the customer as required in the instance where customers failed or refused to submit the required data and information for the verification of their identity and the creation or update of their economic profile.

iv. Ongoing monitoring of customers' accounts and transactions

- CySEC noted that some regulated entities did not provide accurate information on the methods used to monitor account transactions for unusual behavior. This included the insufficient amount of accurate and up-to-date data held on customers, making it difficult to develop parameters for identifying unusual, suspicious transactions without obvious legitimate purpose needed to comply with the Law and Directive.
- On some occasions, regulated entities with a significant number of customers followed a manual risk assessment and transaction monitoring procedure. This raised questions as to their ability to monitor such a large volume of customers sufficiently, continuously and in a timely manner.
- Weaknesses in the procedures implemented by some regulated entities as regards to screening customers on the International Sanctions adopted by the UN Security Council and the Restrictive Measures adopted by the Council of the EU.

v. Internal suspicious reporting and reporting to MOKAS

- CySEC found that some regulated entities did not have adequate and appropriate measures and procedures in place in order to implement:
  - The internal suspicious reporting to the regulated entity's Compliance Officer of any information or other matter which proves or suspects that a customer is involved in money laundering or terrorist financing offences;
  - The examination of the internal suspicious reports by the Compliance Officer and their reporting to MOKAS, when it is established or there are reasonable suspicions that a customer is involved in money laundering or terrorist financing offences.

- CySEC has identified that the number of internal suspicious reports to the Compliance Officer, and in turn reports from the Compliance Officer to MOKAS is relatively low for some regulated entities. Factors taken into consideration included the large number of customers and their respective risk categorisations, the nature and complexity of the products and services provided by the regulated entities, the size of the volume and value of the transactions conducted, the geographical areas of the business activity.

In light of the above, regulated entities must fully comply with the Law and the Directive in place to prevent money laundering and terrorist financing and in the event of non-compliance will be subject to the administrative sanctions available to and enforced by CySEC under the Law.

Sincerely,

Demetra Kalogerou
Chairwoman of the Cyprus Securities and Exchange Commission