

To : **Regulated Entities:**

- i. Crypto Asset Service Providers ('CASPs')**
- ii. Cyprus Investment Firms ('CIFs')**
- iii. Administrative Service Providers ('ASPs')**
- iv. UCITS Management Companies ('UCITS MC')**
- v. Self-Managed UCITS ('SM UCITS')**
- vi. Alternative Investment Fund Managers ('AIFMs')**
- vii. Self-Managed Alternative Investment Funds ('SM AIFs')**
- viii. Self-Managed Alternative Investment Funds with Limited Number of Persons ('SM AIFLNP')**
- ix. Companies with sole purpose the management of AIFLNPs**
- x. Small Alternative Investment Fund Managers ('Small AIFMs')**

From : **Cyprus Securities and Exchange Commission**

Date : **8 August 2024**

Circular No : **C656**

Subject : **Common weaknesses/deficiencies and good practices identified during the inspections performed in relation to the prevention of money laundering and terrorist financing**

The Cyprus Securities and Exchange Commission ('CySEC') wishes, with this circular, to inform the Regulated Entities the following:

During 2022 and 2023, CySEC performed inspections of its Regulated Entities to assess their compliance with the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007, as amended ('the Law') and CySEC's Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing, as amended ('the Directive').

From the inspections performed, CySEC has already outlined the measures that the specific Regulated Entities should implement to ensure full compliance with their AML/CFT requirements. To support improvement across all Regulated Entities' AML/CFT systems and

controls and to set expectations, CySEC shares some examples of good practices applied across Regulated Entities, as well as some weaknesses/deficiencies commonly identified during these inspections, which are summarized below:

A. Consolidated good practices

CySEC identified the following good practices when carrying out its inspections:

- The use of, where available, local knowledge and open-source internet checks to supplement commercially available databases when researching potential high-risk customers including politically exposed persons ('PEP').
- Clear processes for escalating the review/approval of high risk and all PEP customer relationships to senior management.
- The conduct of face-to-face meetings and discussions with high-risk and PEP prospects before accepting them as a customer.
- Ensuring customer files contain a customer overview covering risk assessment, documentation, verification, expected account activity, and a profile of the customer or of the business relationship and beneficial owners.
- Transaction & account monitoring which takes into consideration up-to-date customer due diligence ('CDD') information including expected activity, source of wealth and source of funds.
- Monitoring new customers more closely to confirm or amend the expected account activity.
- Involving senior management and AML/CFT staff when considering whether to maintain or terminate high-risk relationships.
- Keeping AML/CFT policies and procedures up to date to ensure compliance with evolving legal and regulatory obligations.

B. Common weaknesses/deficiencies

CySEC identified the following common weaknesses/deficiencies when carrying out its inspections:

1. Risk management and procedures manual for the prevention of ML/TF (the 'Manual')

- i. In some cases, the Manual included a description of the procedures referred to in paragraph 9(1)(c) of the Directive, instead of tailoring those procedures within the Regulated Entity. For example, the customers' acceptance policy, which constitutes a part of the said manual, was on some occasions too general and not prepared after detailed assessment of the risks faced by the Regulated Entity from its customers and/or their transactions and/or their countries of origin or operations, as stated in Part IV of the Directive.

- ii. In addition, there were occasions where although the Regulated Entity accepted cash transactions, the Manual did not include procedures and controls for the purpose of identification and detection of transactions in cash, which may be unusual and/or carry enhanced risk of being involved in money laundering (ML) and terrorist financing (TF) operations.
- iii. Moreover, in some instances the measures and procedures for the detection of actions that are in breach or may potentially be in breach of the Sanctions and Restrictive Measures that are decided and imposed by the United Nations' Security Council and the European Union respectively, were not documented at all or were inadequately recorded in the Manual.

2. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) Measures

- i. In some instances, the Regulated Entities failed to construct and/or update a complete customer economic profile due to failing to collect information on the size and source of income, source of funds and size of wealth as well as to provide detailed description of the customers' main business activities and operations. Failure to construct a complete customer economic profile reduces the ability to monitor the customers' transactions in a satisfactory manner, ultimately increasing the overall ML/TF risk.
- ii. On a few occasions, the Regulated Entities failed to obtain sufficient evidence to ensure the verification of the identity of the beneficial owners, to understand the ownership and control structure of their customers.
- iii. On a number of occasions, although the Regulated Entities had classified customers as high risk, there was lack of supporting evidence to verify that they had obtained additional information for the application of enhanced customer due diligence measures, in addition to the measures referred to in sections 60, 61 and 62 of the Law, thus failing to manage and mitigate sufficiently the associated ML/TF risks.

3. AML/CFT Risk Assessments

- i. In a number of cases, the Regulated Entities, when conducting the customer's AML/CFT risk assessment, failed to take into consideration the EBA's Risk Factors Guidelines, as per paragraph 12(4) of the Directive (CySEC Circular C276) and in the case of the ASPs sector, the Risk-based Approach (RBA) Guidance for Trust and Company Service Providers (TCSPs) adopted by the Financial Action Task Force (FATF) (CySEC Circular C331).
- ii. For business relationships with customers and/or customers' beneficial owners who have acquired Cypriot citizenship, either themselves, or their spouses and/or their children,

under the Cyprus Investment Program (CIP), in some cases, the Regulated Entities have not always accounted for the risks posed by these customers in their AML/CFT risk assessments. As a result, the Regulated Entities did not demonstrate an effective and thorough assessment of the ML/FT risks posed by the said customers, and thus not implementing appropriate CDD measures.

- iii. In some cases, the Regulated Entities failed to flag and properly assess published adverse information, relating to the reputation of their customers and/or beneficial owners and thus failed to assess correctly the customer's risk. Furthermore, merely recording and/or assessing customer's negative information without determining and applying appropriate measures to address the specific adverse information, in terms of CDD, allows for potential ML/TF risks to remain within the services provided by the Regulated Entities.
- iv. On some occasions, the risk assessment form used by the Regulated Entities to assess the customers' ML/TF risk, resulting to the categorisation of customers according to paragraph 7(2)(c) of the Directive, did not include risk factors which are associated with the UN Sanctions and the EU Restrictive Measures.

4. Source of funds and Transactions Monitoring

- i. On a number of occasions, the Regulated Entities failed to collect supporting documentation of the customer's transactions conducted, in order to ensure that a satisfactory audit trail was maintained. Specifically, as regards to the ASPs sector, it has been identified that in some cases, the Regulated Entities had only provided a brief description, prepared by its staff, to support/justify the transactions carried out instead of obtaining evidence of the relevant transactions.
- ii. In a few cases, the Regulated Entities obtained insufficient supporting documentation of the customers' initial source of funds. In particular, the following relevant points should be taken into consideration by the Regulated Entities:
 - In cases where customers are legal entities, and when loans are provided as evidence of the source of funds, the Regulated Entities should examine factors and obtain evidential information including that of the lender and the relation with the customer, the terms of the loan and the reason for providing the loan and evidence of whether the loan is repayable as well as evidence of the source of funds of the lender. The same approach should apply when the customer provides loans to other entities. In another example, the existence of funds/financial assets kept in a client account for a long time, does not release the Regulated Entity of the obligation to keep an updated customer economic profile to monitor the customer's transactions by tracing the source of funds and wealth at early stages. Additionally, the transfer of financial assets or portfolio of investments to another Regulated Entity, does not release the latter from its duties to obtain all necessary information from the customer for the

construction of a complete and up-to-date customer economic profile, including the initial source of funds.

- On the same note, obtaining information, for example audited financial statements of the customers, may not always be sufficient evidence of their source of funds. Regulated Entities should obtain further information and supporting evidence in cases where the source of funds cannot be evidenced/supported from the audited financial statements as well as examine whether the information obtained is proportionate to the customer's economic profile.
- Moreover, in cases where the ASPs provide directorship services, the obligation to identify and obtain evidence of the source of funds of the transactions executed for/by their customers remains in place.

5. Reporting of suspicious transactions/activities to the Unit for Combating Money Laundering ('MOKAS')

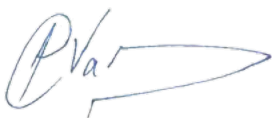
In some cases, compliance officers of Regulated Entities failed to examine internal reports in the light of all relevant available information for the purposes of determining whether the information or other matter contained in the said report proves or creates a suspicion that a person is engaged in a money laundering offence or terrorist financing, and if so to report this immediately to MOKAS.

6. Record Keeping

In a number of cases, the Regulated Entities did not ensure that documents and information referred to in section 68(1) of the Law, were promptly and without delay made available to CySEC for the purpose of execution of its duties, as provided in section 68(2) of the AML/CFT.

CySEC expects all Regulated Entities to carefully consider the contents of this Circular and take the necessary steps to gain assurance that their policies, controls, and procedures are commensurate with their risk profile and comply with the relevant legal and regulatory requirements. In addition, CySEC wishes to remind Regulated Entities, that in the event of non-compliance, they will be subject to the administrative sanctions available to and enforced by CySEC under the Law.

Sincerely,



Panikkos Vakkou

Vice Chairman, Cyprus Securities and Exchange Commission