ΕΠΙΤΡΟΠΗ ΚΕΦΑΛΑΙΑΓΟΡΑΣ ΚΥΠΡΟΥ
CYPRUS SECURITIES AND EXCHANGE COMMISSION

To : **Regulated Entities**
i. CIFs
ii. ASPs
iii. UCITS Management Companies
iv. Internally managed UCITS
v. AIFMs
vi. Internally managed AIFs
vii. Internally managed AIFLNPs
viii. Companies with sole purpose the management of AIFLNPs

From : **Cyprus Securities and Exchange Commission**

Date : **February 28, 2019**

Circular No : **C 299**

Subject : **Guidance on Identifying, Assessing and Understanding the Risk of Terrorist Financing in Financial Centres**

Further to the release of the ***Guidance on Identifying, Assessing and Understanding the Risk of Terrorist Financing in Financial Centres*** ('the Guidance') in January 2019 which was examined and endorsed by Moneyval Committee of the Council of Europe at its 56th Plenary meeting, the Cyprus Securities and Exchange Commission ('the CySEC') issues the following as a summary of its findings:

In recognition of the fact that there is limited information available internationally about the use of formal financial systems for terrorist financing (TF) purposes, international TF experts and representatives from a number of financial centres (FCs), took part in a workshop to consider the specific TF risks facing FCs and the information they should draw on for the purpose of identifying, assessing and understanding these risks.

The conclusions from the workshop were set out in the said Guidance for the participating jurisdictions to use in assessing their TF risks and to assist other jurisdictions that may face similar challenges, in furtherance of the global fight against TF.

The Guidance has been prepared on the basis that the primary TF risk for most FCs is likely to arise from their use as transit jurisdictions for the movement of funds linked to terrorist activity outside the jurisdiction, or from their involvement in the management of foreign funds or businesses that are linked to such activity. Specifically, according to the Guidance, the more likely exposure to TF for FCs arises from their high levels of cross border business, particularly

complex transactions and the international activities of their charities and other non-profit organizations (NPOs) with the attendant possibility of the services and products offered by FCs or assets raised and/or disbursed by their NPOs being used by parties outside the jurisdiction to fund terrorism abroad.

An additional consideration when assessing TF risk is the crossover between threat and vulnerability as it is not possible fully to distinguish between TF threat and the vulnerability arising from products and services being used for TF purposes. The Guidance mentions two aspects for the assessment of the TF threat of a FC:

i. The first aspect is to look at connections between the FC and focus jurisdictions, including the extent to which the FC's businesses or NPOs may be involved in the international movement of goods that could be used for terrorism or to finance terrorist activities.
ii. The second aspect is to consider the extent to which terrorism or TF is occurring in jurisdictions with which the FC has close geographical and/or political links.

The assessment of the TF vulnerability of a FC also contains two aspects:

i. An examination of the extent to which the services or products offered by FCs are likely to be attractive for TF purposes; and
ii. the extent to which the FC has adequate measures in place to address TF.

All Regulated Entities must consider the Guidance, attached to this Circular, in identifying, assessing and understanding TF risks for the implementation of adequate and appropriate policies, controls and procedures so as to mitigate and manage TF risks effectively, as per article 58(a) of the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007.

Sincerely,

Demetra Kalogerou
Chairwoman of the Cyprus Securities and Exchange Commission

Guidance on Identifying, Assessing and Understanding the Risk of Terrorist Financing in Financial Centres

This document was examined and endorsed by MONEYVAL at its 56th Plenary meeting (3-6 July 2018, Strasbourg)

1 Introduction

1.1 Financial centres (**FCs**), like all jurisdictions, can only put in place effective measures to address terrorist financing (**TF**) if they fully understand their risks in this area. For reasons looked at below, the primary TF risk for most FCs is likely to arise from their use as transit jurisdictions for the movement of funds[1] linked to terrorist activity outside the jurisdiction, or from their involvement in the management of foreign funds or businesses that are linked to such activity.

1.2 Assessing these types of TF risk presents particular challenges. In addition to the obvious difficulties inherent in assessing risks related to activity elsewhere, to date international attention has tended to be focused more on the (typically small-scale) funds required to carry out specific terrorist attacks than on large-scale funds held by terrorist organisations that may not be linked to a specific attack, and only limited information is available internationally about the use of formal financial systems for TF purposes. In addition, like most jurisdictions, FCs have little or no TF case experience to draw on.

1.3 In recognition of this, representatives from a number of FCs and some international TF experts took part in a two-day workshop in Monaco in April 2018 to consider the specific TF risks facing FCs and the information they should draw on in order to identify, assess and understand these risks.

1.4 This document sets out the conclusions from the workshop in the form of guidance for the participating jurisdictions to use in assessing their TF risks going forward. It is envisaged that it may be made more widely available in order to assist other jurisdictions (including jurisdictions which are not FCs) that may face similar challenges, in furtherance of the global fight against TF.

2 Background

2.1 Any assessment of TF risk must consider each of the three widely recognised methods of TF, namely collection, movement and use of funds. For many jurisdictions, the process of identifying, assessing and understanding the risk of each of these methods primarily involves looking at previous cases of terrorism by individuals or organisations that are either within, or linked to, the jurisdiction in question (e.g. members of a diaspora), and examining the financial needs of these individuals or organisations in order to draw conclusions about the methods of TF most likely to be used.

2.2 However, the demographic and geographical factors typically applicable to FCs[2] make it unlikely that acts of terrorism will have taken place within their borders, or will have been carried out elsewhere by individuals or organisations that have residential, familial or other social links to them. While the geographic position of some FCs puts them at risk of being used as a transit country for people transporting physical assets (e.g. pre-paid cards) for TF purposes, for most their geographical position means that

---

1 References to funds includes assets or resources of any kind.

2 Different considerations apply to FCs that are located within a large country facing specific terrorist risks, or that are close to conflict zones, or where a sizeable section of the population has ethnic, religious or historical links to areas likely to be affected by terrorism.

this possibility is remote. Similarly, for FCs without a significant manufacturing and trade sector, import and export of goods that could be used for terrorist purposes or used to finance terrorist activities is unlikely, although the possibility of FCs being used as transit countries for such goods should not be overlooked (especially in the case of FCs that are free ports or with ports which have significant entrepot activity with a range of other jurisdictions).

2.3 Clearly no FC can rule out being exposed to these forms of activity, and must, like any other jurisdiction, look at the available national security etc. information to assess its TF risks in this respect. However, the more likely exposure to TF for FCs arises from their high levels of cross border business, particularly complex transactions, and the international activities of their charities and other non-profit organisations (collectively, **NPOs**), with the attendant possibility of the services and products offered by FCs or assets raised and/or disbursed by their NPOs being used by parties outside the jurisdiction to fund terrorism abroad. Therefore, although FCs cannot ignore collection and use of funds when identifying, assessing and understanding TF risk, their principal focus will be on cross-border activity involving the movement of funds. Broadly speaking, this is likely to occur in one or more of the following ways:

2.3.1 flow-through, i.e. where the FC is used as a transit country for funds intended for use in foreign terrorism;

2.3.2 service provision, i.e. where funds relating to terrorism do not enter the FC but where businesses in the FC provide administration or other services to parties that support foreign terrorism – these could be internationally active domestic or foreign entities, politically exposed persons (**PEPS**) or high net worth individuals;

2.3.3 the use of complex structures involving legal persons and legal arrangements to disguise the underlying beneficial owner who may be involved in terrorism or TF, or feature on a terrorism related sanctions list;

2.3.4 abuse of philanthropy, i.e. where donations or aid that are sent or administered from the FC go to conflict zones, either directly or via internationally active domestic or foreign NPOs, and are diverted to support foreign terrorism; and

2.3.5 use of funds generated by illicit activities (money laundering) to finance terrorism.

2.4 Statistics and underlying information directly indicating these forms of TF (e.g. previous investigations or prosecutions, suspicious activity reports relating to TF, intelligence reports of TF from domestic or foreign agencies, requests for assistance in TF cases from other jurisdictions (e.g. mutual legal assistance or Financial Intelligence Unit requests which include TF related information), or assets frozen under terrorism-related United Nations Security Council Resolutions[3] (collectively, the **UNSCRs**)) are likely to be the most valuable sources of information for assessing the relevant risks. However, the

[3] UNSCRs 1267, 1373 and successor UNSCRs.

experience of most FCs is that they have seen none, or very few, of these indicators to date. It is recognised that, given the internationally accepted difficulties in detecting TF, it cannot simply be assumed that the absence of these indicators means that FCs are not being used for TF purposes. Instead, it means that FCs must look at other sources of information in order properly to assess their TF risks.

2.5 An additional consideration for FCs when assessing TF risk is the crossover between threat and vulnerability. Because their most significant TF threat arises from their products and services being used for TF purposes by individuals or organisations anywhere in the world that have no other link with the jurisdiction, it is not possible fully to distinguish between this threat and the vulnerability arising from those products and services. For this reason, some of the factors looked at below in the context of threat are also relevant to assessing vulnerability[4].

3 Information relating to threat

3.1 The assessment of the TF threat of a FC has two aspects.

3.2 The first is to look at the extent of any connection between the FC and focus jurisdictions (i.e. jurisdictions that present a higher risk of terrorism or which have strong geographical or other links with such countries), including the extent to which the FC's businesses or NPOs may be involved in the international movement of goods that could be used for terrorism or to finance terrorist activities.

3.3 The following categories of information are relevant to this aspect:

3.3.1 data on flows to and from the FC by jurisdiction. The available flow data will vary from FC to FC, but is likely to include information on the following:

3.3.1.1 bank deposits;

3.3.1.2 correspondent banking;

3.3.1.3 investments;

3.3.1.4 use of ATMs abroad to withdraw funds from accounts within the FC;

3.3.1.5 wire transfers to and from the FC;

3.3.1.6 loads and spends in respect of pre-paid cards;

3.3.2 the extent to which any of the following categories of person are from focus or high risk jurisdictions or linked to such jurisdictions:

[4] Consequence is not looked at in this guidance, as it is not considered to present any issues that are specific to FCs.

3.3.2.1 the beneficial owners of domestic legal persons or legal arrangements, or of foreign legal persons or legal arrangements administered domestically, including NPOs;

3.3.2.2 relatives or associates of beneficial owners of domestic legal persons or legal arrangements, or of foreign legal persons or legal arrangements administered domestically, including NPOs;

3.3.2.3 people exercising control over domestic legal persons or legal arrangements, or over foreign legal persons or legal arrangements administered domestically, including NPOs;

3.3.2.4 people with links to domestic legal persons or legal arrangements or to foreign legal persons or legal arrangements administered domestically, including NPOs (e.g. joint ownership of property);

3.3.3 the extent to which assets held by and activities undertaken by domestic legal persons and legal arrangements, or by foreign legal persons or legal arrangements administered in the FC (including NPOs), are located in focus jurisdictions or linked to such jurisdictions;

3.3.4 the extent to which business relationships and one-off transactions are carried out with parties who are in or are linked to focus jurisdictions (including foreign NPOs that may otherwise have no nexus with the jurisdiction), and the features and characteristics of those relationships or transactions; it is important to be aware that TF involves small and large sums, with large sums typically more likely to arise in relationships or transactions with PEPs or other persons that are involved in state-sponsored terrorism or with larger terrorist organisations;

3.3.5 the extent to which assets or activity linked to the FC have been identified as subject to international sanctions imposed on focus jurisdictions; as indicated above, for most FCS these are unlikely to relate to TF, but they are still relevant to assessing TF because they are additional indicators of the likely extent of links in general between an FC and focus jurisdictions;

3.3.6 the extent to which focus jurisdictions, or individuals or entities from or linked with focus jurisdictions, feature in suspicious activity reports, intelligence reports or requests for assistance from other jurisdictions received by the FC; the point made immediately above about the relevance of international sanctions cases applies equally here;

3.3.7 the extent to which financial or administration services are provided from the FC in respect of the import or export of goods or other trading activity that could be used for terrorism or to finance terrorist activities;

3.3.8 the features and characteristics of domestic NPOs, especially the zones of activity for those that operate abroad and the extent to which this includes focus jurisdictions (here it is important to be aware that NPOs may change their

focus and purposes over time, and that there may be possible TF within donations or other transactions between domestic NPOs);

3.3.9 the features and characteristics of any overseas aid provided by a domestic authority, especially its zones of activity and the extent to which this includes focus jurisdictions; and

3.3.10 the extent to which the FC is used by foreign PEPs (in light of the possible link with state-sponsored terrorism).

3.4 It is important to bear in mind that, as customers frequently use more than one FC for the purposes of a particular structure or transaction, links with focus jurisdictions may not be immediately apparent. This is less likely to be an issue where the data being considered is focused on an underlying customer, as the due diligence process if properly applied should reveal the relevant link. However, where flow data is being looked at, i.e. where the information solely relates to a source or destination jurisdiction, if that jurisdiction is another FC acting as an entrepot, the FC in question will be recorded as the source or destination even though the relevant assets have come from, or are intended for, a third jurisdiction. In order to see beyond entrepot FCs to the jurisdictions likely to be behind them, it will be necessary for an FC to form an assessment of the type of jurisdictions that use the other FCs which feature prominently in its flow data. This will require looking at evaluation reports and risk assessments relating to those FCs, international cooperation requests from them or involving them and media information about them (e.g. the Panama Papers). It may also involve liaising directly with their authorities.

3.5 The second aspect is to consider the extent to which terrorism or TF is occurring in jurisdictions with which the FC has close geographical and/or political links. This could include internet research, reviews of the evaluation reports and risk assessments of those jurisdictions, meetings with relevant authorities and other formalised arrangements.

4 Information relating to vulnerability

4.1 The assessment of vulnerability also has two aspects.

4.2 The first is an examination of the extent to which the services or products offered by FCs are likely to be attractive for TF purposes. In the absence of any relevant domestic case experience, this will primarily involve looking at external sources of information such as:

4.2.1 international or regional typologies on TF;

4.2.2 evaluation reports of other jurisdictions offering similar services, products or customer profiles;

4.2.3 risk assessments produced by other jurisdictions with similar services, products or customer profiles, and relevant supranational risk assessments;

4.2.4 information on TF patterns provided at authoritative outreach events (e.g. presentations at MONEYVAL, the FATF, by the UNODC, by the IMF or by the World Bank); and

4.2.5 information about business relationships between FCs and parties linked to terrorism from media sources, including data leaks such as the Panama Papers.

4.3 The second is the extent to which the FC has adequate measures in place to address TF. In the absence of TF case experience, this will involve considering the following matters:

4.3.1 whether there are any gaps in the preventive or repressive legal frameworks that may make it difficult to prevent, detect, investigate or prosecute TF; deficiencies in the framework governing customer due diligence are particularly likely to be relevant here;

4.3.2 the extent to which the authorities, private sector and NPOs have a good understanding of TF; this should include recognition of the fact that larger terrorist organisations require large sums to fund their activities;

4.3.3 the extent to which there is a sufficient skill base to investigate terrorism and TF and supervise compliance with TF requirements;

4.3.4 the extent to which formalised arrangements with other jurisdictions are operating effectively at operational and policy level;

4.3.5 the findings of authorities (the regulators or registrars as the case may be for financial services businesses, DNFBPs or NPOs) about the extent to which preventive measures are complied with;

4.3.6 the extent and effectiveness of any action taken by the authorities to enforce the preventive regime;

4.3.7 the extent of the cross-border physical movement of funds that takes place in or from the FC;

4.3.8 the findings of the competent authority (or authorities) for implementation of international sanctions, or oversight of such implementation, about the extent to which they are complied with; although as indicated above there may not be any experience, or limited experience, of implementing the UNSCRs, the level of compliance with similar measures may be relevant to the likely compliance with the UNSCRs (as this may demonstrate whether reporting entities generally look beyond the obvious to uncover links to sanctions targets);

4.3.9 the extent and effectiveness of any action taken by the authorities to enforce international sanctions; this is relevant for the reason given immediately above;

4.3.10 the extent and circumstances in which cash and other services and products that facilitate anonymity and that are increasingly known to be linked to TF (e.g. prepaid cards and virtual or crypto-currencies) are offered by or used within the FC; change(s) in the pattern of offering or use; and the ways in which they might be offered or used within the FC for TF;

4.3.11 the extent to which the authorities, private sector and NPOs have a good understanding of Fintech, Regtech, block chain and other developing technologies; relevant changes to these technologies; and the way(s) in which they might be offered or used within the FC for TF; and

4.3.12 the extent to which any sectors, products or services that were identified in the threat assessment feature in money laundering cases (i.e. previous investigations or prosecutions, suspicious activity reports, intelligence reports from domestic or foreign agencies, requests for assistance from other jurisdictions); to be clear, this is to identify possible shortcomings in the FC's regime to address money laundering which could also be relevant to its ability to address TF.