UIFAND
UNITAT D'INTEL·LIGÈNCIA FINANCERA D'ANDORRA

INFORMATIVE NOTE ADDRESSED TO THE BANKING FINANCIAL SECTOR REGARDING THE PREVENTION OF, AND FIGHT AGAINST, TERRORIST FINANCING

Date: 28 June 2019

Purpose: Compilation of recommendations regarding the prevention of, and fight against, terrorist financing (TF).

Rationale

The National Risk Assessment adopted by Andorra in December of 2016 determines that there is a moderate ("medium-low") level of risk of **terrorist financing** for the country as a whole, **focused mainly on activities involving the attraction and movement of funds**. Consequently, measures should be taken which will allow precautions to be enhanced so that the financial system, and especially the banking sector, will not be used to attract funds from other jurisdictions with the aim of transferring such funds to third countries for terrorist purposes.

In the exercise of its supervisory function, UIFAND has carried out in this respect a **thematic inspection that covers the entire banking sector** of Andorra, in order to assess the degree of effectiveness of the internal control systems and control procedures, addressed specifically to the prevention of, and fight against, terrorist financing, that the entities have in place.

In this connection, a check has been made to determine whether the entities have in place the most basic internal controls in this field; these controls should have the following purpose:

(i) verification of customers and/or counterparts of customers, in United Nations sanctions lists;

(ii) analysis of the transactions of customers in high-risk countries or areas of special concern;

(iii) assurance that the transfers of funds contain the minimum information required in Chapter 5 of *Law 14/2017, of 22 June, on prevention and the fight against the laundering of money or assets and terrorist financing* (hereafter Law 14/2017);

(iv) analysis of the products that allow disposal of cash abroad; and

(v) identification of business relations with non-profit organizations.

As a result of the on-site thematic inspections which we have carried out, UIFAND is issuing this informative note, which contains a series of **recommended actions**, with the aim of helping reporting entities to mitigate the risks inherent to terrorist financing.

General considerations on the prevention of terrorist financing

First of all, it is necessary to specify a series of conceptual aspects relating to the detection of, and the fight against, terrorist financing.

The **prevention of terrorist financing** is not limited only to the five points listed in the preceding paragraph, inasmuch as the implementation of controls in this field is a necessary but not sufficient requirement to ensure effective action.

Accordingly, the prevention of terrorist financing includes a set of **conducts, typologies and indicators** which require the existence of **suitable detection and management mechanisms**. A significant document on conducts of this type is the latest publication, issued by UIFAND on 14 December 2018, on terrorist financing typologies.

Within this framework, it is important to mention the differences, of both conceptual nature and with respect to obligations, between the **detection of activities connected with the laundering of money or assets, the detection of activities connected with terrorist financing, and the adoption of restrictive measures:**

1) *Terrorist financing and laundering of money or assets*

Firstly, some of the elements which usually serve to define conceptually the transactions susceptible of involving the **laundering of money or assets** include the following:

- The **origin of the funds** is always **illegal**; the funds come from **criminal activities** and/or criminal organizations.
- Such transactions are mainly **channelled** through the **regulated financial system**.
- These transactions are usually **detected** through **suspicious transactions** which do not fit in with the expected wealth or transactional activity of the customer.
- The **amount** of the respective **transactions** is usually **large** and such transactions are often **fractioned** with the aim of avoiding the obligations of reporting and/or of adopting due diligence measures.
- Such transactions usually involve **complex international networks** which include the use of front companies, bearer shares and/or offshore jurisdictions.
- The **traceability of the funds** is **circular**, that is to say, they usually return to the person who generated them, they are returned to the financial system, or they are reused for future criminal laundering transactions.

In contrast, **terrorist financing** activities are characterized by the following features:

- The **origin of the funds** may be either **legal or illegal**, coming from the self-financed terrorist cells themselves, which are centred around criminal activities, or externally through donors, benefactors or fund-raisers.

- Such funds are commonly **channelled** through courier services, cash withdrawals by means of the use of credit cards, sending and **physical transport of money** and/or other **informal financial systems** such as *hawala* or "currency exchange houses" (foreign companies whose main purposes are foreign currency exchange and international transfers of funds).

- Likewise, such activities are usually **detected** through **suspicious relations**, such as transfers of funds between parties who do not appear to have any apparent relationship.

- The **transactions** characteristically involve **small amounts**, usually below the thresholds for which obligations are established for reporting, declaration, or adoption of due diligence measures.

- The **financial activities** that characterize terrorist financing may involve **a number of methods**, ranging from the regulated financial system to other informal systems for transmission of assets or the smuggling of goods or cash.

- The **traceability of the funds is linear**, that is to say, the funds which have been generated or raised are intended for the promotion of terrorist activities and groups.

Consequently, although the criminal activities of laundering of money or assets and those of terrorist financing are usually mentioned together, and even though they have some points in common, the types of cases in which they occur are clearly distinct.

This reflection has been necessary since, although the differences and points in common between these two concepts are generally known, there is a general tendency amongst reporting entities to use the same control systems to detect both of these conducts, as is highlighted in Point 1.1 of this document, thereby reducing the capacity of detection and, therefore, the effectiveness of such control systems.

2) Terrorist financing and adoption of restrictive measures

Secondly, it is important to bear in mind the differences between the aim of the **verifications against the consolidated list of the United Nations Security Council** and the **detection of terrorist financing activities.**

In this respect, if the consultation of this list proves positive, this circumstance **does not constitute a suspicion but rather a certainty**, since the persons and entities contained in the consolidated list of the United Nations Security Council are designated for their links with terrorism, terrorist financing or the financing of the proliferation of weapons of mass destruction, and they require the **application of restrictive measures** (usually the freeze of funds/transactions).

On the other hand, in the event in which activities are detected which are suspected of being related to terrorism or its financing, this circumstance should generate, if appropriate, the submission of a **suspicious transaction report** to UIFAND.

This point is important because it often happens that these two concepts are confused in the formalization of the written protocols of action and written internal control procedures of the reporting entities, for example by attributing the same category to the lists of risk countries and the lists of designated persons and entities.

Accordingly, the reporting entities should make enhanced efforts to set out differently, in their internal control procedures, both the various measures of prevention and

identification of transactions suspected of terrorist financing, and the actions in response to positive cases of designated persons.

For all these reasons, we recommend that consideration should be given to both the aforementioned TF indicators of December of 2018, and the guide for the application of restrictive measures issued by UIFAND in February of 2017.

Lastly, in conclusion to the foregoing reflections, we must insist that **the fight against terrorist financing should not be limited to the identification of persons and entities designated** by the resolutions of the United Nations Security Council but rather, the reporting entities should go beyond the screening of customers and counterparts. This point is important since **designated persons and/or entities do not usually carry out transactions themselves,** but rather they operate through other natural persons and/or legal entities which have no apparent relationship with them, and without at-risk or forbidden countries or jurisdictions necessarily being involved.

In order to detect cases of such activities, it is essential to possess as much knowledge as possible with respect to the control structure and the beneficial owner of the customer, and also with respect to the originators and the beneficiaries of the transactions in the case in which the provision of a transaction intermediation service is involved.

Recommended improvement actions to mitigate the risks inherent to terrorist financing

Just as has been previously stated, the following improvement actions relating to various risk factors of terrorist financing, without being of compulsory compliance, seek to provide support to the reporting entities and especially to those belonging to the banking financial sector, in order to raise the level of effectiveness of their controls for detection and prevention of conducts susceptible of involving terrorist financing.

1. General considerations about control systems

1.1. Specific controls for detection of terrorist financing

- **The reporting entity should have an in-depth knowledge of the implemented tools and controls**, and of their respective purposes (that is to say, what type of transactions they are intended to detect and with what aim). This knowledge includes, in the case of warning systems, the scenarios in which the tool would provide warning for a subsequent analysis, and the various parameterization criteria (data on which the analysis is based, type of transaction, period analysed, etc.), among others.
- You should review the **parameterization** and the criteria linked to the general ML/TF controls so that they will ensure effective detection of conducts associated with TF, reviewing the amounts, volumes and typologies of the transactions that these controls take into consideration.
- New scenarios should be developed in the warning systems to ensure specific detection of conducts and typologies such as those listed in the latest document on TF risk indicators published by UIFAND.
- The scope of the analysis that is to be carried out in the **management of warnings** should be clearly established, and it should be understood to include the procurement of information and/or documentation that explains the consistency

between the respective transaction or group of transactions that have caused the warning to be issued, and to include a comprehensive knowledge of the customer.

- A periodic assessment should be made of the **effectiveness of the warning systems**, and this assessment should take into consideration, as a minimum, the number of warnings analysed, the various actions carried out by the persons in charge of the management of warnings, and the suspicious transaction reports submitted to UIFAND as a result of this control.

1.2. Documentary justification of the analyses carried out in connection with the control systems

- Objective criteria should be defined with respect to the **granting of hierarchical authorizations** of transactions, and the aforementioned analyses should be documented in order to ensure that these authorizations are granted on the basis of documents, data or information obtained from reliable independent sources.
- The procedure for application of continuous follow-up measures of business relations should be reviewed, specifically in relation to the scrutiny of transactions, in order to require that, in all the risk scenarios defined by the entity which involve transactions and/or movements of funds in high terrorist-risk areas, the **analysis** will be carried out on the basis of documents, data or information obtained from reliable independent sources.

1.3. Availability of sanctions lists

- Control systems should be implemented that ensure the detection of any **update of the sanctions lists**, especially including the consolidated list of the United Nations Security Council, and that ensure the correct implementation of the sanctions lists in the systems as soon as such updates occur, instead of making periodic downloads.

  It should consequently be ensured that customers are always verified against the most up to date version of such lists, ensuring that restrictive measures are immediately applied, when appropriate.

1.4. Application of controls of numbered accounts

- **Periodicities of reviews** to be performed against the sanctions lists should be established for account-holders and intervening parties of numbered accounts and transactions carried out from numbered accounts; such periodicities of review should allow the detection, as soon as they arise, of cases to which it is necessary to apply measures immediately, as in the case of restrictive measures.
- It should be ensured that the risk classification and the grading of the measures based on the identified risk are established by taking into consideration the overall assessment of the customer, that is to say, by taking into account, in an aggregate way, the respective customer's positions in named accounts and in numbered accounts.

2. *Specific controls of transfers of funds*

2.1. Sanctions screening / verification against sanctions lists by other means

- **A procedure should be implemented** that ensures that a record is made of all the transactions subjected to the system of verification against sanctions lists (for example, Swift Sanctions Screening), and that a record is made of the results of the controls carried out. The documentary record of the control should also include the transactions that have not given a positive result, even if the characteristics of the system do not allow such a record to be made in an automated way for reasons of limitations of the historical file or others.
- Implemented procedures should be in place to ensure that the verifications against sanctions lists are carried out **before the issue or the payment of the transfe**r, and that such procedures cover both the originator and the beneficiary, in all cases.
- In the cases in which "white lists"[1] are on hand, a formal procedure should be established for the inclusion of persons in such lists, and a periodic review of such persons should be established against all the sanctions lists, in order to ensure detection of any possible change with respect to the initial situation, that has allowed such persons to be included in the list.

2.2. Information on the originator/beneficiary, which accompanies the transfers of funds

- A **procedure should be implemented**, or in the event in which it is already in place, it should be **duly formalized in the protocols of the reporting entity**, with the aim of ensuring that the customer is informed as the beneficiary of the transfer, and of verifying the accuracy of such information, regardless of the amount of the transfer (that is to say, also for transfers under 1,000€) before the sending or the payment into account of the transfer.
- The controls should be reviewed in order to ensure that they allow detection of the absence of the name of the originator or of the beneficiary in the form of meaningless information (for example, chains of random characters or clearly erroneous designations), without this implying a manual review of all transfers.

3. *Specific controls of cash withdrawals*

- Consideration should be given to the introduction of freezes or prohibitions of cash withdrawals and the use of **credit cards** in the jurisdictions near conflict areas or areas with terrorism risk.
- Systems should be developed to control the transactions of **cash withdrawals and payments in commercial establishments abroad**, especially in the jurisdictions or regions sensitive to terrorism risk which UIFAND and/or the reporting entity have determined as such, reducing the degree of support on the controls carried out by third parties, such as credit card providers.
- The **analysis *ex-post*** which is carried out in relation to the transactions of cash withdrawals and payments in commercial establishments abroad should be focused on both the transaction itself and on the knowledge of the customer in general, and the consistency between the two and other additional factors should be assessed.

[1] *Internal lists that have the purpose of excluding a customer's name from the verification analysis; these lists are usually used in cases of customers with some degree of coincidence with names on the sanctions lists and who present recurrent transactions.*

4. *Non-profit organizations (NPOs)*

- The procedure established to identify business relations between the entity and the NPO should be reviewed. It should be recalled that the risk presented by these organizations is not linked to the circumstance of their being of non-profit character, but rather to their capacity **to raise funds from the general public or to transfer their funds to third parties**.
- **The consideration of NPOs as "high risk" should be justified on the basis of an analysis** that takes into account such factors as their typology, sphere of action, volume of managed funds, or activity (above all with respect to the existence or absence of international transactional activity). Measures should be adopted to ensure that the files of customers in the NPO category contain sufficient documentation to provide a suitable knowledge of these customers, especially with regard to their identification and control structure, and to the origin of the funds which are provided.
- Warning scenarios should be implemented which allow identification of suspicious activities relating to NPOs, such as the typologies mentioned in the UIFAND Technical Communiqué no. CT-01/2017, issued on 1 March.

5. *Other considerations. Understanding of customers' risks*

5.1. Understanding of the activity of legal-entity customers

- A field should be added to the customer's **KYC** which clearly states whether the legal-entity customer is an active company or not in terms of whether or not it carries out a commercial activity. This statement should be verified against reliable documentation or information (consultation of the Register of Commerce, on-site visit to the customer's facilities, etc.). The follow-up measures of the transactions of customers should also be consistent with this statement and such measures should be documented (financial statements, invoices, etc.).

5.2. Classification of customers' risk level

- An exhaustive effort should be made to establish clear criteria of risk classification that are as uniform and objective as possible.
- The necessary measures should be taken to ensure that the modifications of the **risk level of customers**, especially in the cases in which manual modifications prevail over automatic calculation, cannot be carried out without the need for their justification or without a record being made of the analysis that is carried out to justify them.