



FINANCIAL INTELLIGENCE ANALYSIS UNIT

**GUIDANCE NOTE**

**ON**

**FUNDING OF TERRORISM – RED  
FLAGS AND SUSPICIOUS ACTIVITIES**

*A GUIDANCE NOTE ISSUED BY THE FIAU ON RED FLAGS AND SUSPICIOUS  
ACTIVITIES THAT MAY BE INDICATIVE OF FUNDING OF TERRORISM*

**Issued: 7 February 2018**

## **Background Information**

1. Funding of terrorism consists in making funds or other assets available to terrorists and/or terrorist organisations to support them in their operations. The terrorist attacks which have taken place of the past years have highlighted the negative and destabilising consequences terrorism can have if left unchecked. Disrupting the financial channels of terrorists and terrorist organisations is one way in which to combat this phenomenon as the absence of funds limits their operational ability.
2. One of the objectives that the Prevention of Money Laundering and Financing of Terrorism Regulations 2017 ('the PMLFTR') seeks to achieve is combatting the funding of terrorism. Subject persons play a key role in ensuring that the financial and/or other systems are not misused to fund terrorism. To this end, subject persons who know, suspect or have reasonable grounds to suspect that a transaction may be linked to funding of terrorism have to report the same to the Financial Intelligence Analysis Unit ('the FIAU') as set out under Regulation 15(3) of the PMLFTR. Given the current regional and global scenario, the FIAU wishes to remind subject persons of their obligations under the PMLFTR and assist them in this regard.
3. The FIAU is issuing this Guidance Note to provide subject persons with a list of red flags or suspicious activities that may point to funding of terrorism. No single red flag is a clear indication that funding of terrorism is or may be taking place. Subject persons however have to consider the occurrence of any red flags on a case-by-case basis within the context of the services and products they offer as well as what they know about their customers and their activities (e.g. the customer's declared activity, his source of funds, the transaction's background etc.).

## **Funding of Terrorism – Red Flags/Suspicious Activities**

4. The following is an indicative list of common funding of terrorism indicators which subject persons should take into consideration in determining whether they have the required knowledge, suspicion or reasonable grounds to suspect that funding of terrorism is taking place:
  - i. Acquiring, or changing smaller denominations into, large denomination currencies that are internationally accepted (Euro, USD etc.), especially, but not only, if this is known to coincide with travelling arrangements to areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support.
  - ii. The transfer of funds:
    - a. To or from areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support, without any legitimate or reasonable explanation for the said transfer(s). Particular attention should be made to transfers of funds to the same beneficiary account but with the recipient indicated with different names.

- b. To or from entities that, though not subject to any international or EU sanctions, are known to be sympathetic to, or have links with, terrorist groups.
  - c. To or from individuals and/or entities involved in the informal financial sector (e.g.: *hawala*)
  - d. Including references that may indicate extremist beliefs or short suspicious messages.
- iii. Payments related to the acquisition of substances and materials that are not related to, or in quantities that are unusual for, the individual's known activities and can be used in the construction of explosive devices (e.g. acquisition of aluminium pipes, fertilizer, scrap iron etc.).
  - iv. Payments related to travelling arrangements to or from areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support or payments made in relation to communication services provided in these areas.
  - v. Bank account activity conducted remotely (e.g. through on-line banking, ATMs, debit/credit cards etc.) from areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support. Particular vigilance should be exercised where such remote access coincides with the receipt or transfer of significant sums of money or if this follows a period of prolonged account inactivity.
  - vi. Using e-wallet and/or stored value/pre-paid cards in areas where terrorist groups are active, or in close proximity thereto, or to areas where terrorist groups are known to enjoy support.
  - vii. Taking out personal loans which are drawn down but the debtor defaults thereon and the creditor is not able to enforce its rights against the debtor or even communicate with the same.
  - viii. Liquidating personal assets (e.g. selling one's residential home, liquidating any retirement plans, withdrawing all funds in bank accounts, etc.).
  - ix. Donations to voluntary organisations having connections with geographical areas where terrorists are active or in close proximity to the same, or to voluntary organisations that are known or suspected to have been infiltrated by terrorists.
5. Subject persons are hereby reminded that:
- i. The list provided hereabove is not exhaustive and a customer may exhibit other indicators that he may be involved in funding of terrorism.
  - ii. They are not to provide services to or facilitate the transfers of assets involving individuals and/or entities that are subject to international or European Union

sanctions. It is therefore important that they screen their client base regularly against lists of sanctioned individuals and entities as well as whenever updated or new lists are issued. Subject persons are to *inter alia* refer to Section 3.7 of Part I of the Implementing Procedures issued by the FIAU.

- iii. Atypical activity by a customer may be a sign of money laundering and/or funding of terrorism. However, given that in the case of funding of terrorism a transaction's value may be significantly lower than usual, the application of thresholds for on-going monitoring purposes may limit a subject person's ability to detect them. Thus, when carrying out on-going monitoring, subject persons are also to consider low value transactions which may or may not be accompanied by one or more of the red flags listed above.
  - iv. Any risk assessment carried out by subject persons, as well as any measures, policies, controls and procedures adopted by them in terms of Regulation 5(5) of the PMLFTR, are to also consider funding of terrorism risks. Direct or indirect links with areas known for terrorist activity and/or support and/or activities known to be used by terrorist groups to finance themselves should receive due consideration whenever a risk assessment is carried out.
  - v. They are to keep abreast of developments so as to be aware of which jurisdictions are exposed to terrorism or are suspected of supporting terrorists and terrorist organisations. A jurisdiction can be considered as supporting terrorists and terrorist organisations independently of whether any such support is provided by state authorities or private individuals.
6. Subject persons are also encouraged to enhance their knowledge on the subject in question by attending training and reading relevant material published by various bodies, including for example, publications made available by the FATF and other international or regional bodies as indicated in the Annex to this Guidance Note.

### **Questions and Queries**

7. Any questions or clarifications in relation to the contents of this Guidance Note may be addressed to:

The Director  
FIAU  
65C, Tower Street  
Birkirkara, BKR 4012

Email: [info@fiumalta.org](mailto:info@fiumalta.org)

## ANNEX I

### Financial Action Task Force (<http://www.fatf-gafi.org/>)

- i. Financing of Recruitment for Terrorist Purposes – January 2017
- ii. Emerging Terrorist Financing Risks – October 2015
- iii. Financing of Terrorist Organisation Islamic State in Iraq and the Levant – February 2015
- iv. Risk of Terrorist Abuse in Non-Profit Organisations – June 2014
- v. The Role of *Hawala* and Other Similar Service Providers in Money Laundering and Terrorist Financing – December 2013