

31 October 2023

## The Israeli - Palestinian Conflict Guidance Note

### I. Introduction

Recent developments in Israel and the Gaza Strip have once more brought to the fore the issue of financing of terrorism ('TF'). Terrorist organisations, networks and even lone actors need assets and funds to function and carry out their activities.

TF is often presented, explained and addressed together with money laundering ('ML'). However, the two are quite distinct one from the other. Unlike ML, the funds and assets involved in TF may have been derived legitimately and the concern of those involved is more often than not to conceal the destination, rather than the origin, of the funds and assets. The amounts involved may also be quite small compared to what may be encountered when it comes to ML. There are some similarities between the two, in that funds and assets involved may also be the proceeds of criminal activity. This requires not only concealing the end recipient but also the origin of any such funds and assets. Some ML-techniques can be used to achieve both ends.

What needs to also be borne in mind is that TF is not only about funds and assets being used for the carrying out of terrorist attacks but about making funds available to terrorist organisations, networks and lone actors for whatever purpose. Whether the financing is then used to acquire explosives, run hospitals, corrupt officials or manage schools is irrelevant as it still constitutes TF.

The international and European communities make use of a number of tools to stifle TF, including international sanctions, restrictive measures and counter-financing of terrorism ('CFT') obligations ('CFT').

The Malta Financial Services Authority ('MFSA') and the Financial Intelligence Analysis Unit ('FIAU') are issuing this Guidance Note to remind subject persons of their obligations in relation to TF and to especially draw their attention to the potential risks emanating from the current situation in Israel and the Gaza Strip. Specifically, the intention behind this Guidance Note is to remind all subject persons of their obligations under the National Interest (Enabling Powers) Act<sup>1</sup> ('NIA') and of how sanctions may impact subject persons' obligations under the Prevention of Money Laundering and Funding of Terrorism Regulations<sup>2</sup> (PMLFTR) and the FIAU Implementing Procedures.

---

<sup>1</sup> Cap 365 of the Laws of Malta.

<sup>2</sup> Subsidiary Legislation 373.01.

## II. Geopolitical Context

Reports on the on-going conflict have been replete with references to Hamas. Hamas, officially the Islamic Resistance Movement, is a political and militant Islamist movement which operates within the Occupied Palestinian Territories, which is designated as a terrorist group by the United States<sup>3</sup> and the European Union (EU)<sup>4</sup>. This entails that it is subject to restrictive measures imposed by the EU, including the freezing of all funds and other financial assets it may have, hold or otherwise dispose of within the EU. Any sanctions or restrictive measures imposed by the EU are directly applicable and enforceable in Malta under the local legislative sanctions' regime.

Despite being subject to sanctions and being cut off from the international banking system, Hamas still manages to exercise control over the Gaza Strip as well as organise, coordinate and conduct attacks which require significant amounts of financial resources<sup>5</sup>. The use of shell companies, the abuse of non-profit organisations as well as the use of virtual financial assets ('VFAs') and precious metals have allowed Hamas to still gather the necessary financing to carry out its activities, circumventing sanctions and restrictive measures.

How can subject persons abide by sanctions and leverage any synergies between the two regimes to better counter TF?

## III. Obligations under the NIA

Every subject person has an obligation to ensure that applicable sanctions imposed on any entity or individual are adhered to. Particular attention must be paid to any assets that may be subject to freezing in terms of these sanctions and to the obligations arising from Article 17 of the NIA in relation to the same.

Furthermore, subject persons are reminded of their additional obligations under Article 17 (6) and Article 17 (7) of the NIA and, specifically, to their obligations to:

- Promptly informing the Sanctions Monitoring Board (SMB) about any identified targeted assets and the actions taken by the subject person concerning them. Additionally, any attempts to engage in transactions involving identified targeted assets should also be reported to the SMB.
- Establishing and maintaining robust internal controls and procedures to ensure compliance with their sanction screening obligations and effectively implementing these controls in their day-to-day operations.

---

<sup>3</sup> Hamas was designated as a Foreign Terrorist Organization (FTO) by the United States on 08 October 1997.

<sup>4</sup> Hamas is listed in the Council Implementing Regulation (EU) 2022/147 of 3 February 2022 implementing Article 2(3) of Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.

<sup>5</sup> European Parliament resolution on the despicable terrorist attacks by Hamas against Israel, Israel's right to defend itself in line with humanitarian and international law and the humanitarian situation in Gaza (2023/2899(RSP)).

- Regularly checking the relevant sanctions lists and conducting regular screenings of their client database against the same. This screening should extend to both existing and potential customers. Subject Persons are reminded that any update or revision to sanction lists is to be considered as a trigger event for an immediate re-evaluation of one's client database.
- Avoiding disclosure to any customer or third party regarding freezing measures undertaken in accordance with the NIA.

In implementing measures to comply with these obligations, subject persons are to refer to any guidance issued or otherwise made available by the SMB. As part of its efforts to ensure that all interested parties are duly informed about relevant developments on sanctions, the SMB runs a notification service. Subject persons are encouraged to subscribe to the same by sending an email on [updates.smb@gov.mt](mailto:updates.smb@gov.mt).

In addition, subject persons should keep abreast of the latest developments with regards to reported trends and typologies when it comes to TF. Given the nature of the sanctions being referred to in this document, these same trends and typologies are likely to be used to circumvent sanctions aimed at restricting access by terrorist organisations, networks and lone actors of funds and assets to finance their activities. Relevant documentation with which subject persons are to familiarise themselves include:

- The FIAU's Guidance Note on the Funding of Terrorism.
- The FIAU's Guidance Note A Look Through the Obligation of Transaction Monitoring.
- EUROPOL's EU Terrorism Situation and Trend Report.
- The FATF's Report on Emerging Terrorist Financing Risks.

A number of other bodies make available information on accounts and VFA addresses that they have identified as being linked to TF. These should also be taken into consideration to assess whether there have been any attempts at sanctions circumvention. Subject persons should be especially vigilant when servicing entities or individuals that have links to areas known for terrorist activities as they may very well be acting as a front for TF. In such instances, the risk of sanction circumvention as well as TF are especially high and subject persons should satisfy themselves as thoroughly as possible that any funding collected and made available is not being used for TF.

In this context, the Regulation (EU) 2015/847 acquires particular importance. Known also as the Funds Transfer Regulation, the said instrument imposes a number of obligations on subject persons who provide payment services, including ensuring that any transfer of funds is accompanied by relevant information on the identity of the transfer's originator and beneficiary. In addition, payment service providers also have obligations to ensure that the information accompanying the transfer of funds is complete and does not contain any misleading or incorrect information. This can be an especially important tool to therefore identify transfer of funds (and as of 30 December 2024 even VFA transfers) that may be taking place in violation of sanctions.

#### **IV. AML/CFT Obligations and Sanctions**

The implementation of sanctions and restrictive measures can influence how subject persons adhere to their AML/CFT responsibilities, especially when conducting Customer Due Diligence ('CDD') procedures. There is a potential overlap where the data gathered for AML/CFT compliance purposes may also be valuable in ensuring the accurate enforcement of sanctions and restrictive measures. This is especially true when it comes to TF as the subject person has to adhere to two regimes that are intended to address the same phenomenon.

The following are some key areas where there can be synergies between the AML/CFT and sanctioning regimes but where additional attention should also be exercised by subject persons:

##### **1. Understanding and Evaluating Risk**

In the process of assessing the risk of ML/FT, subject persons need to factor in how they may be abused to circumvent sanctions, in this case intended to address the phenomenon of TF. Subject persons need to assess whether the products and/or services they offer present any vulnerabilities that may be exploited by ill-intentioned actors to circumvent sanctions and make funds and other resources available to terrorist organisations, networks and lone actors. And this is especially true where the service or product can be abused to obfuscate the end recipient of any such funds and resources.

Subject persons have to also consider whether jurisdictions with which their customers have links are areas where designated terrorist organisations, networks or lone actors are known to operate or are otherwise known to sympathise with any such organisations, networks or lone actors.

The imposition of sanctions and restrictive measures directly influence the risk of ML/FT linked to a customer or, if relevant, their beneficial owner(s). The introduction of such measures necessitates a re-evaluation of the overall risk assessment for existing business relationships and plays a pivotal role in proactively determining the risk associated with the onboarding of a prospective customer. It is also imperative to closely scrutinise information acquired through adverse information screening, particularly when it associates a prospective customer or beneficial owner with an individual/entity subject to sanctions or restrictive measures.

##### **2. Beneficial Ownership**

The implementation of sanctions and restrictive measures might encourage beneficial owners targeted by these sanctions to disassociate themselves from the entities or legal arrangements they have a stake in. This also applies to any individuals who suspect that they might themselves eventually become subject to similar sanctions or restrictive measures. Subject persons should be vigilant in discerning whether such efforts to relinquish beneficial ownership are sincere or simply an attempt to mask the identity of the actual beneficial owner, while the initial beneficial owner maintains control over the entity or arrangement through alternative means.

When engaging new customers and conducting screening for any adverse information, subject persons should place specific emphasis on any finding that could connect the customer or the beneficial owner to a sanctioned individual/entity or someone with a high likelihood of being sanctioned. If credible and recent information of this nature comes to light, subject persons should exercise increased scrutiny to determine whether the individual requesting their services or who is otherwise declared as the customer's beneficial owner, is acting on behalf of someone else.

### 3. Transaction Monitoring, Scrutiny and Reporting

During the process of transaction monitoring and scrutiny, subject persons should consider any activities or transactions that suggest a customer may be violating sanctions. Special attention must be directed towards customers known to have significant interactions with countries where terrorists are active or known to sympathise with terrorists' views, or those who maintain close ties with individuals or entities subject to such sanctions or restrictive measures. This holds true both in relation to single transactions and, especially in the area of TF, to transactional patterns. There is therefore a need for subject persons to identify any such transactions and scrutinise the same to assess whether there are any links to TF and sanction circumvention.

In addition to any reporting obligations mandated by the NIA or other applicable laws in Malta, subject persons have to bear in mind their own reporting obligations under Regulation 15 of the PMLFTR. In the case of sanctions intended to target TF, the reporting obligation is triggered due to two factors:

- a. The circumvention of sanctions restricting terrorists' access to funds and assets could in itself amount to an instance of TF that is reportable in terms of Regulation 15(3).
- b. The breach of legally binding sanctions constitutes a predicate offence. Any proceeds linked to such activities should therefore be regarded as gains from criminal conduct, necessitating the submission of a Suspicious Transaction Report under Regulation 15(3) of the PMLFTR.

In this context, subject persons are specifically reminded of their responsibilities under Regulation 15(4) of the PMLFTR to abstain from executing such transactions until an STR is submitted to the Financial Intelligence Analysis Unit (FIAU), and the statutory review period by the FIAU has lapsed. Subject persons are to make use of the appropriate template submitting any such report to the FIAU through goAML as this will assist the FIAU in identifying the reports that need to be prioritised.

### 4. Effective Leverage of Sanction Information for Transaction Monitoring Purposes

It is worth noting that in the realm of AML/CFT, reference is not only being made to those sanctions and restrictive measures which are legally binding and enforceable under the Maltese law through the NIA but also includes those imposed by other jurisdictions such as the United Kingdom via the Office of Financial Sanctions Implementation (OFSI), the United States through the Office of Foreign Assets Control (OFAC), and various other jurisdictions. Whilst these alternative sanctions and restrictive measures may not be legally binding under Maltese law, they influence the implementation of AML/CFT measures by subject persons.

In a number of instances, these alternative sanctions and restrictive measures include account details and VFA addresses that have been identified as being linked or controlled to terrorist organisations. This has already happened with Hamas and this information can be especially relevant in the context of transaction monitoring. All of the said information can help identify attempts by subject persons' customers to transfer funds and assets to terrorist organisations, networks and lone actors. It also allows a subject person receiving and/or remitting funds and assets to assess whether its services were somehow used in the past to carry out TF in which case any such instance should be reported to the FIAU.

**V. Conclusion**

Subject persons should remain mindful of the significance of adhering to relevant sanctions and fulfilling their screening and freezing obligations as mandated by the NIA. They should also ensure compliance with the AML/CFT obligations set forth in the Prevention of Money Laundering and Funding of Terrorism Regulations and the FIAU's Implementing Procedures in an area as sensitive as TF. As can be seen from the above, the AML/CFT and the sanctioning regimes may present overlaps but there are also several synergies between the two which, if used wisely, can ensure a more effective application of one's obligations and strengthen the fight against terrorism.