TARGETED FINANCIAL SANCTIONS

TYPOLOGIES OF TF-RELATED TARGETED FINANCIAL SANCTIONS
- MARCH 2023 -

CONTENTS

INTRODUCTION

1. The United Nations (UN), through its Security Council Resolutions (UNSCRs) and Sanctions Committees, aims to maintain peace and security, by mandating the implementation of freezing measures related to terrorism and terrorist financing (TF). By adopting resolutions aimed at blocking terrorists' and terrorist organizations' disposal of their financial assets, the objective of TF-related targeted financial sanctions (TFS) is to curtail the movement of payments and capital related to terrorism.

2. The Principality of Monaco (Monaco), as a member of the UN, is committed to implementing the sanctions measures imposed by the UNSCR. This commitment spreads over all UN sanctions regimes, thus including the implementation of measures ranging from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions.

3. However, natural and legal persons designated on UNSCRs use sanction circumvention tactics to strategically evade the sanctions imposed on them. As such, Monaco is committed to protecting its financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) from abuse by illicit actors engaging in terrorist financing and sanctions evasion.

4. Given the intricacies related to the identification of sanction circumvention tactics, this document presents cases and examples on how these sanctioned activities, persons, groups, or entities have received financing and support, therefore violating or evading UNSCRs related to terrorism and terrorist financing.[1] It is of great importance that the entire population of natural and legal persons in Monaco exercises caution and vigilance to ensure that individuals or organizations which are subject to United Nations Security Council (UNSC) TF-related sanctions are in no way supported.

5. This document also includes a list of red-flag indicators that can aid FIs and DNFBPs to detect any suspicious transactions linked to TF-related TFS.

Scope of Typology Paper

6. This typology paper has been issued by the Advisory Committee on the Freezing of Funds and Economic Resources (the Advisory Committee) to assist reporting entities with the implementation of TFS-related obligations. The information contained in this paper does not in any way whatsoever constitute legal advice, and should be read in conjunction with relevant national legislation, international standards, and guidelines issued by the Advisory Committee or other competent agencies (e.g. SICCFIN, DSP).

Contact details

7. For all enquiries, reports and requests associated with the implementation of TF-related TFS please email the Advisory Committee on the Freezing of Funds and Economic Resources.

Email: dbt.geldefonds@gouv.mc

Website: https://geldefonds.gouv.mc/en

[1] The TF-related UNSC Resolutions are UNSCR 1267 (1999) and 1989 (2011) related to the Islamic State in Iraq and the Levant (Da'esh), and Al-Qaida, and UNSCR 1988 (2011) related to the Taliban.

TERRORIST FINANCING

What is Terrorist Financing?

8. The term terrorist financing (TF) includes the provision of funds to commit terrorist activities as well as offering the support and maintenance of the person (terrorist) or the terrorist group. The term encompasses the provision of food, lodging, training, as well as making means, such as transportation or communication equipment, available. Such financing can take place with physical cash, transfers, or in kind contributions. It should be noted that funds involved can be from legal or illegal sources.

9. The International Monetary Fund notes that the primary goal of individuals or entities involved in the financing of terrorism is not necessarily to conceal the sources of the money but to conceal both the funding activity and the nature of the funded activity.

10. The following are methods and cases that illustrate how terrorist groups have misused economic sectors or activities to fund their interests. This document compiles information from documents developed by the UNSC, the United Nations Office on Drugs and Crime (UNODC) and the Financial Action Task Force (FATF).

Terrorist Financing Methods

11. FIs and DNFBPs have faced an ever increasing wall of new legislation and regulatory requirements over the past decades, of which a large proportion focused on the topic of Anti Money Laundering/Countering the Financing of Terrorism (AML/CFT). The general tendency was to assume that AML-related components (incl. red flags and typologies) apply equally to the financing of terrorism.

12. However, real life cases have highlighted that techniques employed by money launderers are drastically different from those involved in terrorist financing. The core reason for the difference is that the objectives of the money launderer and those of the terrorist financier differ enormously. Both criminals need to achieve a disconnect between the source of funds and their entry into the financial system. However, the money launderer seeks to achieve long term benefits from his crime and is prepared to obtain these in a wide variety of forms, while the terrorist financier focuses on providing currency or means to those involved in supporting or committing acts of terrorism.

13. Given this fundamental difference in objectives, the typologies related to TF also differ to those of money laundering. The FATF identified that the Islamic State in Iraq and the Levant (ISIL) earns revenue primarily from five sources:

- illicit proceeds from the occupation of territories, such as bank looting, extortion, control of oil fields and refineries, and robbery of economic assets and illegal taxation of goods and cash that transit territory where ISIL operates;
- kidnapping for ransom;
- donations including by or through non-profit organizations;
- material support such as support associated with foreign terrorists fighters; and
- fundraising through modern communication networks.[2]

14. Similarly, a UN-led report from 2020 (the Joint Report)[3] concluded that the most frequently used channels for terrorist financing are:

- the formal banking system;
- cash smuggling;
- the money services business;
- informal remitters or hawala;

[2] 'Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)', Financial Action Task Force, 2015
[3] 'The Joint Report of the Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) concerning Islamic State in Iraq and the Levant (ISIL) (Da'esh), Al-Qaida and the Taliban and associated individuals and entities on actions taken by the Member States to disrupt terrorist financing, prepared pursuant to paragraph 37 of UNSCR 2462 (2019)', United Nations Security Council, 2020

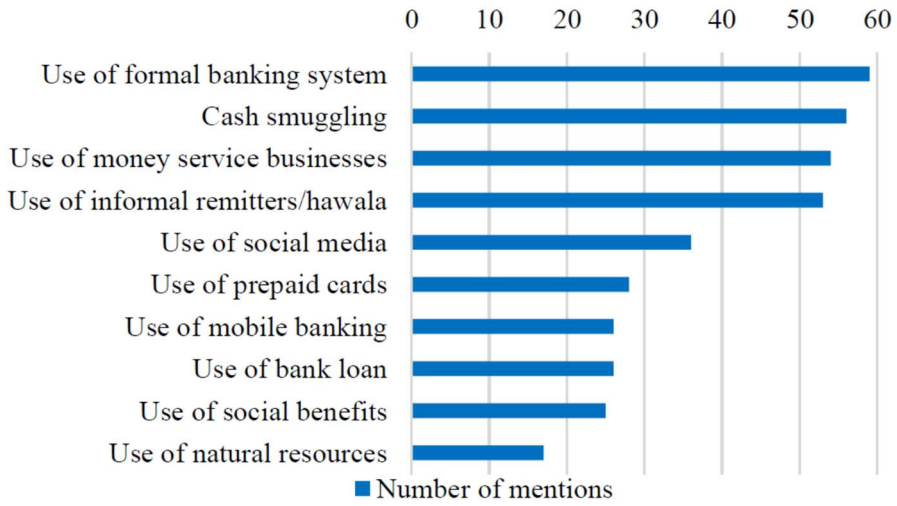
- donations including by or through non-profit organizations;

15. A further human factor which has also had an impact on TF typologies, highlighted by the 9/11 *ex post facto* analysis of hijackers and their actions in the US banks, is that there have been some incidents where suspected individuals engaged in terrorist financing have been pinpointed by alert banking staff due to small actions of abnormal behavior, such as:

- indifference to the actual balance during substantial withdrawals;
- abnormal preoccupation with speed time of transfer, whilst transferring the amounts in several phases to the same destination; and
- an apparent basic lack of knowledge by the depositor/transferor of the destination(s) themselves

16. The Joint report also underlines the abuse of technology (including social media, prepaid cards and mobile banking) for terrorist purposes, noting that TF has been facilitated by recent developments in mobile payments and the anonymity of money transfers and illicit donations via crowdfunding platforms.

17. The graph below gives an overview of the most frequently used methods that terrorist financiers have made use of[4]:



[4] Ibid.

TERRORIST FINANCING – CASE STUDIES

18. The following section will shed light on real-life cases of TF cases that occurred in different sectors, with the goal to increase awareness about these sanctions and the importance of their implementation.

Banking Services

19. The formal banking system is vulnerable to TF because of the difficulty of distinguishing between legitimate and illegitimate low-cost transactions and detecting indirect transactions. Transaction-monitoring programs are often unable to identify terrorism financing. There is also a risk in the use of bank loans and social benefits paid through banks for TF.

Case Study 1: Continued Access to Bank Accounts by Foreign Terrorist Fighters

20. According to sensitive financial information, TF risks were discovered regarding foreign cash withdrawals via ATMs that were made in areas located near territories where ISIL operates by unknown individuals. These withdrawals were taken from US-based bank accounts using a check card. Another TF risk identified was the existence of large deposits into bank accounts followed by immediate foreign cash withdrawals also in areas close to ISIL operational territories. This information revealed the TF risks posed by the continued ability of the individuals who are believed to have travelled to areas occupied by ISIL to reach their bank accounts in their home countries.

Money Remitters

21. Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to TF. In countries where access to banking services is limited, remittance providers may be the primary financial institution through which consumers can engage in cross-border funds transfer activities. Remittance providers are especially vulnerable to abuse for TF where they are unregulated, not subject to appropriate AML/CFT supervision or where they operate without a license (thus operating without undergoing AML/CFT controls).

Case Study 1: A Complicit MSB Agent

22. An individual raised funds for Al-Shabaab from within the Somali diaspora in Missouri and other areas. They used a variety of licensed money service businesses (MSBs) with offices in the United States to remit the money to Somalia for general support of Al-Shabaab fighters. The co-conspirator, who worked for one of the MSBs involved, helped the individual avoid leaving a paper trail by structuring transactions into low dollar amounts and by using false identification information. The MSB worker and other conspirators used fictitious names and phone numbers to hide the nature of their transactions.

Online Payment Facilities

23. Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Funds transfers are often made via electronic wire transfer, credit card, or alternate online payment facilities. Online payment facilities can be vulnerable to identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes, and auction fraud.

Case Study 1: Fundraising via the Internet

24. Intelligence information indicates that some individuals associated with ISIL have called for donations via Twitter and have asked the donors to contact them through Skype. The donors would be asked to buy an international prepaid card (e.g., a credit for a mobile line or to purchase an application or other program which stores credit) and send the number of the prepaid card via Skype. The fundraiser would then send the number to one of his followers in a country close to Syria and sell the number of the card with a lower price. The remaining cash would then be brought to an ISIL member.

Case Study 2: Use of PayPal Accounts for Fundraising

25. In France, a charity was set up in 2010, whose chairman was specialized in e-marketing. The charity offered several options on its website to make donations by credit card, PayPal, cash transfers, or checks. Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below EUR 500. Of the EUR 2 million collected, EUR 600 000 came from a few PayPal transactions from another country. Personal PayPal accounts were also used to collects funds, only to then be withdrawn by cash, or transferred to other accounts.

Case Study 3: Use of Online Financial Accounts for Fundraising

26. Profits from stolen credit cards were laundered by a person in the United Kingdom via several means, including transfer through e-gold online payment accounts. These accounts were used to route the funds through several countries before reaching their intended destination. The laundered money was used both to fund the registration by the criminal of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. Approximately 1,400 credit cards were used to generate roughly £1.6 million of illicit funds to finance terrorist activity.

Donations by or through Non-Profit Organizations

27. Individuals and organizations seeking to fundraise for terrorism and support extremism may attempt to disguise their activities by claiming to be engaged in legitimate charitable or humanitarian activities and may establish non-profit organizations (NPOs) for these purposes.

Case Study 1: Supporting the Recruitment of Foreign Terrorist Fighters

28. Al Rehmat Trust, an NPO operating in Pakistan, was designated pursuant to US Executive Order (EO) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organizations. Al Rehmat Trust was found to be serving as a front to facilitate efforts and fundraising for a UN-designated terrorist organization, Jaish-e Mohammed (JEM). After it was banned in Pakistan in 2002, JEM, a UNSCR 1267 designated Pakistan-based terrorist group, began using Al Rehmat Trust as a front for its operations.

29. Al Rehmat Trust had provided support for militant activities in Afghanistan and Pakistan, including financial and logistical support to foreign fighters operating in both countries. In early 2009, several prominent members of Al Rehmat Trust were recruiting students for terrorist activities in Afghanistan. Al Rehmat Trust has also been involved in fundraising for JEM, including for militant training and indoctrination at its mosques and madrassas.

30. As of early 2009, Al Rehmat Trust had initiated a donation program in Pakistan to help support families of militants who had been arrested or killed. In addition, in early 2007, Al Rehmat Trust raised funds on behalf of Khudam-ul Islam, an alias for JEM.

Case Study 2: Diversion of Funds to NPOs

31. An individual (Mr. A) established a charitable foundation under the pretext of collecting donations for Syrian refugees, people in need of medical and financial aid, and construction of mosques, schools and kindergartens. However, Mr. A was the leader of an organized scheme in which donations were sent to a group of individuals related to Mr. A (Group A) instead of the foundation's account.

32. In most cases, the first stage involved money being sent through money remitters and then transported in cash. The money was then transferred either to credit card accounts or to e-wallets. The members of Group A placed the relevant information (that funds are being collected for the declared purposes) on the internet, but the funds were being sent as an aid for terrorists and their families and meant to be used as financial support for terrorist activities.

33. This information was discovered through investigations conducted by the country's financial intelligence unit (FIU) based on regular monitoring of entities on their domestic list of designated terrorist entities and related persons or on information provided by law enforcement agencies. Analysis of the collected information allowed the FIU to identify the relation between different cases, including common payers and recipients and similar modus operandi in collection and distribution of funds.

34. Further cooperation with law enforcement authorities allowed the FIU to establish the direct link between Mr. A and ISIL activity. This resulted in several criminal investigations related to Mr. A. In addition, Mr. A was listed on the country's domestic list of designated terrorist entities. Assets of Group A members were also frozen.

Smuggling of Cash

35. Cash continues to be a prevalent aspect of terrorist operations. While funds may be raised in several ways, they are often converted into cash that is then taken to conflict zones. This is assisted by porous national borders, difficulty in detecting cash smuggling (particularly in the small amounts that are sometimes smuggled for TF purposes), and the existence of informal and unregulated economies.

Case Study 1: Cash Couriers

36. Over a period of three consecutive days, three individuals declared a total amount of roughly EUR 90,000 in cash to customs officials at the airport in Brussels. The funds were said to originate from NPO A from Germany as part of humanitarian aid in Burundi, Benin, and Zimbabwe. The three couriers were all Belgian nationals and had been living in Belgium for a long time.

37. A Belgian coordinating body of a radical Islamic organization transferred money to accounts held by the three individuals. Over a one-year period, approximately EUR 20,000 was withdrawn in cash, and EUR 10,000 was transferred to Turkey. According to the German FIU, NPO A was one of the largest Islamic organizations in Germany. NPO A was said to be linked with NPO B, which had been banned in Germany for allegedly supporting a terrorist organization. All of NPO B's board members also played a significant role in NPO A.

38. According to information from the Belgian intelligence services, the three individuals referenced above were known to be involved in local branches of a radical Islamic organization. Given the nature of the transactions and the links between the two NPOs, Belgian authorities suspected that at least part of the funds could have been used to support terrorist activities.

Virtual Currencies

Case Study 1: Using Bitcoin for Donations

39. Financial investigations into the terror attack perpetrated by the Christchurch Mosque shooter in New Zealand in 2019 found that shooter had made multiple donations to extreme right wing entities overseas, including Generation Identitaire in France and Martin Sellner in Austria. The references used for these donations were marked as 'gift' and 'keep up the good work'. Additionally, Bitcoin was used for the transfer of funds.

40. The shooter was found to be engaged with 'like-minded' individuals via social media, chatrooms and forums.

Case Study 2: Promoting Virtual Currencies for TF

41. In 2015, Ali Shukri Amin was sentenced to 11 years in prison, followed by a lifetime of supervised release and monitoring of his internet activities for conspiring to provide material support and resources to ISIL.

42. Amin pleaded, admitting to the use of social media platforms to provide advice and encouragement to ISIL and its supporters. He used his social media handle @Amreekiwitness to provide instructions on how to use Bitcoin to mask the provision of funds to ISIL.

43. Amin's social media account boasted over 4,000 followers and was used as a pro-ISIL platform during the course of over 7,000 communications. Specifically, Amin used his account to conduct conversations on ways to develop financial support for ISIL using virtual currency and ways to establish a secure donation system or fund ISIL.

TF-RELATED TFS RED FLAGS

44. The following list provides a non-exhaustive list of potential red flag indicators for TF-related TFS evasion that can aid FIs and DNFBPs to detect any suspicious transactions related to TF:

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk jurisdictions.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Funds are sent or received via international transfers from or to higher-risk jurisdictions.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk jurisdictions.
- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk jurisdictions.
- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk jurisdictions.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk jurisdictions.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk jurisdictions when there appears to be no logical business reasons for dealing with those jurisdictions.
- Transactions involving certain high-risk jurisdictions, such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations, which are subject to weaker AML/CFT controls.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Client donations for causes that are subject to derogatory information that is publicly available