

Terrorist Financing

Typologies and Facilitators



A Strategic Analysis Report

May 2025



Disclaimer

All findings and contents of this report are the property of the United Arab Emirates Financial Intelligence Unit (UAEFIU) or the concerned entities credited as the provider of the data employed in this document. You may not reproduce, distribute, duplicate, alter, create derivative works, or make any modification in any form to exploit or change this document's content and identity.

For any enquiries regarding this document, please contact rsas@uaefiu.gov.ae.

TABLE OF CONTENTS

LIST OF ACRONYMS	iv
EXECUTIVE SUMMARY	v
ILLUSTRATIVE SUMMARY	vi
1. INTRODUCTION	1
2. OBJECTIVES	3
3. METHODOLOGY	4
4. UNDERSTANDING TERRORIST FINANCING	5
5. OVERVIEW OF GLOBAL TERRORIST FINANCING TYPOLOGIES	8
6. EMERGING TYPOLOGIES AND UTILIZATION OF SOPHISTICATED TECHNOLOGIES	10
7. OVERVIEW OF TF NATIONAL RISKS AND LEGAL FRAMEWORK.....	11
8. ANALYSIS OF TF-RELATED STRS/SARS	12
9. IDENTIFIED TF TYPOLOGIES AND TRANSACTIONAL PATTERNS	14
9.1. Movement and obscuring of funds through financial institutions	14
9.2. Movement of funds through unlicensed Hawala	14
9.3. Establishment of corporate networks to move and obscure terrorist funds	15
9.4. Movement of Funds through trade-based terrorist financing (TBTF).....	15
9.5. Trading in high-value items and goods to generate funds	15
9.6. Misuse of the real estate sector	15
9.7. The misuse of virtual assets in crowdfunding and movement of funds	15
9.8. Crowdfunding through local accounts and foreign NPOs	16
9.9. Movement and obscuring of funds through settlement of loans	16
9.10. Movement of funds through high-risk jurisdiction or neighbors.....	16
9.11. Potential illicit funds and other financial crimes as source of funds	16
10. ROLE OF TF FACILITATORS AND INTERMEDIARIES	17
10.1. Designated and listed individuals and entities	17
10.2. Political extremists and high-risk jurisdictions of terrorism	17
10.3. Family members	17
10.4. Money mules	17
10.5. Corporate nominees	17
10.6. Lawyer, accountants, and corporate service providers.....	18
11. DEVELOPED RISK INDICATORS	18
12. CONCLUSION	24

LIST OF ACRONYMS

AML	Anti-Money Laundering
CTF	Counter-Terrorist Financing
FATF	Financial Action Task Force
FIs	Financial Institutions
FIUs	Financial Intelligence Units
FTF	Foreign Terrorist Fighter
IEMS	Integrated Enquiry Management System
IRFI	Inward Request for Information
ISD	Inward Spontaneous Dissemination
LP	Legal Person
MENA	Middle East and North Africa
ML	Money Laundering
MSBs	Money Service Businesses
NPOs	Non-Profit Organizations
NP	Natural Person
PEPs	Politically Exposed Persons
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
UAE	United Arab Emirates
UAEFIU	UAE Financial Intelligence Unit
UN	United Nations
UNSC	United Nations Security Council
UNSC – CTC	United Nations Security Council – Counter Terrorism Committee
UNSC – CTED	United Nations Security Council – Counter Terrorism Committee Executive Directorate
VASPs	Virtual Asset Service Providers

EXECUTIVE SUMMARY

Terrorists need funding to carry out their activities, such as planning, training, recruitment, logistics and acquiring essential materials with which to execute their acts of terror. Disrupting terrorists' and extremists' funds is globally recognized as an essential factor in limiting terrorist organizations' growth and survival. As such, financial institutions (FIs), designated non-financial businesses and professions (DNFBPs), and virtual asset service providers (VASPs) have a significant role in detecting and tracing suspicious transactions and activities relevant to the financing of terrorism.

The effectiveness of Financial Action Task Force (FATF) recommendations relevant to terrorist financing and financing of proliferation (Recommendations 5-8) requires countries to put measures in place that ensure that terrorist financing (TF) activities are investigated and actors who finance terrorism are prosecuted and subject to adequate and proportionate sanctions. In this way, terrorist financing threats are detected and disrupted, terrorists are deprived of resources, and those who finance terrorism are sanctioned. Thereby, such measures enable the prevention of terrorist acts. These are in addition to FATF Recommendation 1, which requires the assessment of money laundering and TF risks at both national and institutional levels. Indeed, the criminalization of TF acts and understanding and identifying TF's risks, including relevant typologies and indicators, are essential in disrupting and weakening terrorist organizations' networks.



















The UAE Financial Intelligence Unit (UAEFIU) conducted a comprehensive strategic analysis of TF-related data available within its databases during the period spanning **01/01/2021 to 31/12/2024**. The analysis work included close examination of 397 Suspicious Transaction Reports (STRs)/Suspicious Activity Reports (SARs)¹ reported during the reviewed period, 104 cases disseminated to the concerned law enforcement and intelligence authorities, as well as relevant requests received from national authorities and international counterpart FIUs. These were in addition to a wide range of publicly available data, including open sources.







This report offers detailed information on TF patterns in raising, moving, managing, and disguising funds, and underlines UAE sectors' vulnerability to TF and major terrorist organizations' potential threat to the UAE. The analysis also identifies different attributes relevant to the actors and financial facilitators involved in the examined cases.

The report concludes with several risk indicators developed from analyzed data to guide reporting entities as well as law enforcement and intelligence authorities in identifying and investigating TF-related incidents.

¹ Only 199 STRs/SARs were valid and reliable to be used as data points in this analysis. Further details are available in section 8.

ILLUSTRATIVE SUMMARY

Utilized Data		Covering Period 01/01/2021 to 31/12/2024		
 199 STRs/SARs	 104 Cases disseminated to law enforcement and intelligence authorities	 43 Technical reports from the UAEFIU to competent authorities (Based on request)	 90 International intelligence reports	 Open source
Identified Typologies				
<u>Potential Sources of Fund</u>				
 Foreign illicit funds	 Crowdfunding through local accounts and foreign NPOs	 Crowdfunding through cryptocurrency	 Trading in high- value items and goods	 Investment in real estate and other sectors
<u>Movement, Management, and Obscuring of Funds</u>				
 Movement of funds pattern through high-risk jurisdictions or neighbors	 Movement and obscuring of funds through financial institutions	 Movement of funds through unlicensed Hawala	 Establishment of corporate networks to move/obscure terrorist funds	 Movement of Funds through trade activities
 Acquisition and successive selling of properties	 Movement of funds through cryptocurrency	 Movement and obscuring of funds through settlement of loans		

TF Facilitators and Intermediaries			
			
Designated individuals/entities	Foreign political extremists		
			
Money Mules	Family Members	Corporate Nominees	Lawyers, Accountants, and Corporate Service Providers abroad

FIU

1. INTRODUCTION

Terrorism continues as a global threat with more shifting patterns and typologies as well as evolving challenges recognized in the spread of terrorism to different geographic reaches; as the number of countries with a recorded terrorist incident “increased from 58 to 66 countries in 2024” (Global Terrorism Index, 2025).²

In February 2025, FATF President Elisa de Anda Madrazo reaffirmed in the periodic “No Money for Terror” event that **“Countries must urgently step up their use of financial intelligence. By turning off the tap of money, we can cut off the blood supply of terrorists. Financial Intelligence is fundamental, and on many occasions, it is the only tool that authorities have to tackle leads and stop an attack. It is important that countries develop frameworks that allow intelligence to be shared efficiently [...] The FATF has provided for FIUs, supported by the Egmont Group for the exchange of information; [this is] a key example for the international law enforcement community to learn from and to make sure we get better at sharing this information.”**³

Terrorism is an essentially contested concept⁴ as there is no standard global definition of terrorism rather than the act of terrorism. Article 2 of the United Nations (UN) International Convention for the Suppression of the Financing of Terrorism (1999) determines the objective of terrorism as being to “intimidate a population or to compel a government or an international organization to do or abstain from doing any act.” Therefore, the legal definition of terrorism or the act of terrorism may vary from one jurisdiction to another, but **terrorism is broadly understood as “a method of coercion that utilizes or threatens to utilize violence in order to spread fear and thereby attain political or ideological goals.”**⁵

The FATF has identified the term **terrorist as “any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.”**⁶

Similarly, the term **terrorist organization refers to “any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii)**

² Institute for Economics and Peace (2025) Global Terrorism Index. Available at: <https://www.economicsandpeace.org/reports/>

³ Elisa de Anda Madrazo (2025) No Money for Terror. Video available at:

https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/FinancialCrime/nomoneyforterror.html#:~:text=FATF%20President%20Elisa%20de%20Anda,blood%20supply%E2%80%9D%2C%0she%20said

⁴ Gallie, W. (1955) ‘Essentially contested concepts’, Proceedings of the Aristotelian Society, 56, new series, 167-198. Available at: www.jstor.org/stable/4544562

⁵ UNODC (2018) Education for Justice: University Module Series - Counter-Terrorism (Module 1: Introduction to International Terrorism). Available at: <https://www.unodc.org/e4j/en/terrorism/module-1/index.html>

⁶ FATF glossary. Available at: <https://www.fatf-gafi.org/en/pages/fatf-glossary.html#accordion-a13085a728-item-2634e09013>

participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.”⁷ Accordingly, TF is interpreted as the financing of terrorist acts, and of terrorists and terrorist organizations.

The early global fight against TF was introduced in the aforementioned UN convention, denoting the required steps and preventative measures in tackling the collection and movement of funds for a terrorist act. The convention underlined the characteristics of the funds, regardless of whether they are “direct or indirect through organizations which also have or claim to have charitable, social or cultural goals or which are also engaged in unlawful activities such as illicit arms trafficking, drug dealing and racketeering, including the exploitation of persons for purposes of funding terrorist activities, and in particular to consider, where appropriate, adopting regulatory measures to prevent and counteract movements of funds suspected to be intended for terrorist purposes.”⁸

This was in addition to the United Nations Security Council (UNSC) Resolution 1373 (2001) requiring states to criminalize TF and impose asset freezes. Furthermore, the resolution emphasized that “**all states shall prevent and suppress the financing of terrorist acts** and refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of members of terrorist groups and eliminating the supply of weapons to terrorists.”⁹ FATF Recommendation 5 specified further technical details and obligations in line with the relevant UN instruments to support states in criminalizing TF and effectively implementing counter-terrorist financing (CTF) measures.¹⁰

Article 18 of the UN 1999 convention, in particular, underlined **the role of reporting transactions suspected of stemming from a criminal activity**, including “complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or obviously lawful purpose.” Similarly, the FATF recommendations established the reporting entities’ obligation within the anti-money laundering (AML)/CTF framework to follow a risk-based approach to identify and understand the risks of money laundering and TF, and report suspicious activities to financial intelligence units (R.1, R.5, R.6, R.8, and R.20). Different cases published by the FATF highlighted

⁷ Ibid.

⁸ United Nations (1999) International Convention for the Suppression of the Financing of Terrorism. Available at: <https://treaties.un.org/doc/db/terrorism/english-18-11.pdf>

⁹ United Nations Security Council (2001) Resolution 1373 (2001) / adopted by the Security Council at its 4385th meeting, on 28 September 2001. Available at: <https://digitallibrary.un.org/record/449020?ln=en&v=pdf>

¹⁰ FATF (2016) Guidance on the criminalisation of terrorist financing (Recommendation 5). Available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/criminalising-terrorist-financing.html

the role of reporting entities and FIUs as one of the mechanisms to detect TF (e.g., APG/MENAFATF, 2019).¹¹

Nevertheless, the UNSC Counter-Terrorism Committee Executive Directorate (CTED, 2024) reported that TF flow still has a wider geographical financial footprint today and has notably expanded to regional financial hubs through the development of regional financial networks to generate and move funds potentially used in establishing new terrorist networks in different conflict zones.¹²

Furthermore, the UNSC Counter-Terrorism Committee (CTC, 2021) indicated that “the persistent shortfalls [in the MENA region that] include the lack of trained human resources and IT tools, which hampers the efforts of FIUs to produce and implement strategic analysis on STRs.” The committee also recognized the good practices in Gulf States, including the UAE, in conducting an overall national terrorism financing risk assessment, but also highlighted the need for further in-depth analysis.¹³

This report provides comprehensive strategic analysis of TF patterns in raising, moving, managing, and disguising funds, including identifying UAE sectors’ vulnerability to TF and the threat perceived in major listed global and local terrorist groups. The report concludes with multiple risk indicators developed from analyzed data indicated shortly in the methodology section, aiming to guide the UAEFIU’s stakeholders in detecting, reporting, and investigating TF-related incidents.

2. OBJECTIVES

As part of the Strategic Analysis Plan and in line with the UAEFIU’s efforts to address and identify patterns and typologies of financial crime, the UAEFIU is delivering this report for the following purposes:

- Increase the understanding of TF risks and its identified typologies among the UAEFIU’s stakeholders.
- Identify TF patterns and methods—including sectors’ vulnerability to TF—by examining how terrorist individuals and groups raise, move, manage, and obscure their funds through the UAE financial and trade systems.
- Outline the TF threat observed in major terrorist groups, countries of concern and the potential international links of terrorist groups.
- Explore links among identified terrorist groups for operational investigation.

¹¹ APG/MENAFATF (2019) Social Media & Terrorism Financing Report. Available at: <https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142>

¹² The UN Security Council Counter Terrorism Committee Executive Directorate (2024) CTED Trends Tracker: Evolving Trends in the Financing of Foreign Terrorist Fighters’ Activity- 2014-2024. Available at: <https://www.un.org/securitycouncil/ctc/content/cted-trends-tracker-evolving-trends-financing-foreign-terrorist-fighters%E2%80%99-activity-2014-%E2%80%93>

¹³ United Nations Security Council Counter-Terrorism Committee (2021) Global survey of the implementation of Security Council resolution 1373 (2001) and other relevant resolutions by Member States. Available at: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_1373_gis_2021_advance_unedited_version.pdf

- Develop risk indicators to guide the UAEFIU's stakeholders in identifying and investigating TF-related incidents.
- Review reporting entities' understanding of TF and ability to detect and report TF-related incidents by examining the quality of their reporting and assessing suspicious reports' validity and reliability, thus enabling effective financial intelligence.

3. METHODOLOGY

This report illustrates TF patterns and methods identified by the UAEFIU from **January 2021 to December 2024**. The UAEFIU strategic analysis team drew up different hypotheses on how terrorist groups raise, move, manage, store, and obscure their funds through the UAE financial and trade systems, using preliminary data and insights collected from different publications, CTF training programs, and open-source data. Thereafter, the team proceeded to test them using data available via the UAEFIU databases. This report is compiled using the following data points:

- STRs and SARs related to TF received through the UAEFIU's reporting system during the examined period.
- TF cases disseminated by the UAEFIU to the concerned competent authorities.
- TF cases initiated by the concerned competent authorities through the Integrated Enquiry Management System (IEMS), including assets frozen.¹⁴
- International intelligence received by the UAEFIU from counterpart FIUs, whether spontaneously or by request.
- Open-source data on listed terrorist individuals, entities, and groups (internationally by the UN, domestically by the UAE, as well as by other foreign sanction regimes).
- Open-source data on known and published cases relevant to specific terrorist groups, indicating their methods and techniques in financing their activities.

Due to the nature of the data points used in this analysis, the current report addresses TF from the perspective of organizational financing rather than operational financing that could be linked to the act of terrorism (incidents that occurred or failed attempts). In other words, with the absence of known specific attacks or attempts, the analysis team interprets the data as intelligence on how terrorist groups finance their activities. The findings of this analysis should be combined with further data available with investigative authorities so as to develop further intelligence.

Moreover, and as indicated in the introduction section concerning the problem of terrorism definition, this analysis considers all identified terrorist groups (and affiliates), whether globally by the UN, domestically in the UAE, or individually by other states. The rationale behind this is based

¹⁴ The Integrated Enquiry Management System (IEMS) is established and owned by the UAEFIU to facilitate communication and processing of different requests between domestic competent authorities, regulated financial institutions and the UAEFIU.

on the FATF Interpretive notes (INR 5.12): “Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.”

Accordingly, this analysis is constructed on two premises:

1. A jurisdiction might face a low terrorism risk from a specific group but still face significant TF risks in the form of that group abusing the jurisdiction’s financial system to disguise and move terrorist funds overseas so as to commit an act of terror in another jurisdiction. As such, funds could be moved or passed through a jurisdiction by terrorists to be used elsewhere.
2. An identified terrorist individual or group in another jurisdiction misusing the country’s financial and trade systems still constitutes a national TF risk because TF techniques and methods could spill over to other domestically listed terrorists to follow the same approach and take advantage of identified sectors’ vulnerability.

The scope of this analysis uses the same terms of ‘individual terrorist’ and ‘terrorist organization’ (group) indicated in the introduction section, but also adds the term ‘political extremists’ to refer to politically exposed persons (PEPs) found to have links with terrorist groups listed by foreign sanction regimes. Nevertheless, the analysis scope does not include PEPs or state actors involved in the state of war. Moreover, the findings of this report do not involve ethnically or racially motivated terrorism due to the unavailability of relevant data.

Lastly, it is worth highlighting that, before utilizing the aforementioned data to reach a conclusion, the UAEFIU strategic analysis team conducted data evaluation to assess its validity, reliability, and excluded data deemed to be incoherent enough to construct TF links.

4. UNDERSTANDING TERRORIST FINANCING

Terrorist groups need operational and organizational funds to pursue their goals and spread their ideology. Operational funds include the money needed for perpetrating a specific attack, while organizational funds are the day-to-day funds needed for maintaining the organizational infrastructure, such as training camps, recruitment salaries, propaganda campaigns, and logistics.¹⁵

Recruitment, particularly of new operative adherents and supporters, is one of the core financial factors influencing terrorist groups’ survival and organizational sustainability. While recruitment cost varies from low to substantial based on the organization’s size and structure, terrorist groups need funds to recruit and hire new members and civil experts, produce (printed and online)

¹⁵ Acharya, A. (2009) Targeting terrorist financing. London: Routledge

recruitment materials, and pay for new recruits' expenses, such as travel, accommodation, fake identification documents, and allocation costs, as well as training infrastructure.¹⁶

Terrorist organizations require funds to keep up with sophisticated technologies to improve their ability to recruit new members, spread their ideology, and fundraise.¹⁷ Furthermore, large terrorist organizations fund and back other terrorist groups which cannot collect enough money for their activities.¹⁸

In that sense, although an individual act of terrorism does not necessarily require a large sum of money, financing remains important to the persistence and sustainability of terrorist groups. With that being the case, applying effective CTF measures is vital when it comes to disrupting and deterring terrorists, as such measures aim to isolate terrorists from the formal international financial system and make it challenging for them to collect and move the funds required for their organization's survival. Moreover, according to different officials and academic work, the current CTF regime not only contributes to the disruption of terrorists' funds, but also helps during the investigation process to define terrorists' locations through paper trails and trace the origin of their financial transactions.¹⁹

Terrorist groups rely on various licit and illicit sources to obtain the funds needed for terrorist activities. The interactions between criminals and terrorists have been cited in different academic work and official documents.²⁰ For example, the UNSC CTED (2024) indicated that "some FTFs engaged in criminal activities to raise funds, including theft, fraud or drug dealing."²¹ Similarly, EUROPOL (2024) underlined that the connection between terrorism and organized crime continues to be observed in terrorism and violent extremism typologies, as opportunistic individual connections to provide weapons and services rather than systematic collaborations.²²

¹⁶ FATF (2018) Financing of Recruitment for Terrorist Purposes. Available at: www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html

¹⁷ Rudner, M. (2006) 'Using financial intelligence against the funding of terrorism', International Journal of Intelligence and Counter Intelligence, 19(1), 32-58. Available at: <https://doi.org/10.1080/08850600500332359>

¹⁸ Gunaratna, R. (2002) Inside Al Qaeda: Global network of terror. 2nd edn. London: Hurst & Co.

¹⁹ E.g., National Commission on Terrorist Attacks upon The United States (no date) Complete 9/11 Commission Report. Available at: <https://9-11commission.gov/report/>; Gardner, K. (2007) 'Fighting terrorism the FATF way', Global Governance, 13(3), 325-345. Available at: <http://www.istor.org/stable/27800665>; Zarate, J. (2013) Treasury's war: The unleashing of a new era of financial warfare. New York: Public Affairs.

²⁰ E.g., FATF (2015) Emerging terrorist financing risk. Available at: <http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html>; FATF (2015) Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL). Available at: <http://www.fatf-gafi.org/publications/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html>; Ryder, N. (2015) The financial war on terrorism: A review of counter-terrorist financing strategies since 2001. Abingdon, Oxon: Routledge.

²¹ UNSC-CTED (2024) CTED Trends Tracker Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014 – 2024. Available at: <https://www.un.org/securitycouncil/ctc/content/cted-trends-tracker-evolving-trends-financing-foreign-terrorist-fighters%E2%80%99-activity-2014-%E2%80%93-2024>

²² EUROPOL (2024) European Union Terrorism Situation and Trend report 2024 (EU TE-SAT). Available at: <https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat>

Accordingly, terrorists are known to move funds using methods identical to those employed by money launderers.²³ Nevertheless, terrorists' motives and TF risk indicators differ from those of money launderers.²⁴ "Money Laundering involves the proceeds of criminal activity being put through a circular process which attempts to give those funds a legitimate source. The funds will then pass back to the criminal that created them," while TF does not require the funds to be returned to their origin and those who created them.²⁵

As regards money laundering, once a criminal act has occurred, criminals need to launder their illicit proceeds through three main stages. These stages,²⁶ as shown in **Chart 1**, involve placement of proceeds into the financial sector, layering by moving funds through the financial system to disguise their origin, and integrating the fund into the economy's legitimate sectors. In this way, money is raised through predicate offences before subsequently being moved through formal channels such as financial institutions or trade transactions, or informal channels, such as smuggling of cash. Following this, funds might be moved several times and/or stored in banks, offshore accounts, or virtual assets, to obscure the flows of funds. Eventually, criminals spend their funds and integrate them into the global economy.²⁷

Conversely, different publications, including FATF and MENAFATF, have explained the TF cycle through four major stages:²⁸

1. Raising funds (e.g., through legitimate businesses, crowdfunding and supporters' donations, self-funding, proceeds of crimes, and other sources generated from territories under the control of terrorist groups).
2. Storing funds (e.g., through cash, bank accounts, gold, high-value items, and real estate).
3. Moving funds (e.g., through financial institutions such as banks, money service businesses (MSBs), Hawala service providers, other modern methods such as virtual assets and internet-based payment services, and physical cross-border movement, including cash couriers).
4. Utilizing funds (to finance terrorists' various activities covering operational needs, purchase of materials and devices, logistics support, recruitment, training, salaries and compensation, or to be utilized for a specific act of terror).

²³ FATF (2015) Emerging terrorist financing risk; and FATF-GAFI (2008) Terrorist financing report. Available at: <http://www.fatfgafi.org/publications/methodsandtrends/documents/fatfterroristfinancingtypologiesreport.html>

²⁴ FATF (2019), Terrorist Financing Risk Assessment Guidance.

²⁵ ECOFEL (2025) Counter Terrorist Financing. Available at: <https://learn.ecofel.org/pages/30/homepage>

²⁶ These stages are not necessarily detected in such sequential order or together and would vary among sectors.

²⁷ ManchesterCF-FIU Connect: Terrorist Financing.

²⁸ For example: MENAFATF (2022) Typologies Project Report on The Abuse of NPOs in TF Activities. Available at: <https://www.menafatf.org/information-center/menafatf-publications/typologies-project-report-abuse-npos-tf-activities>; ECOFEL (2025).

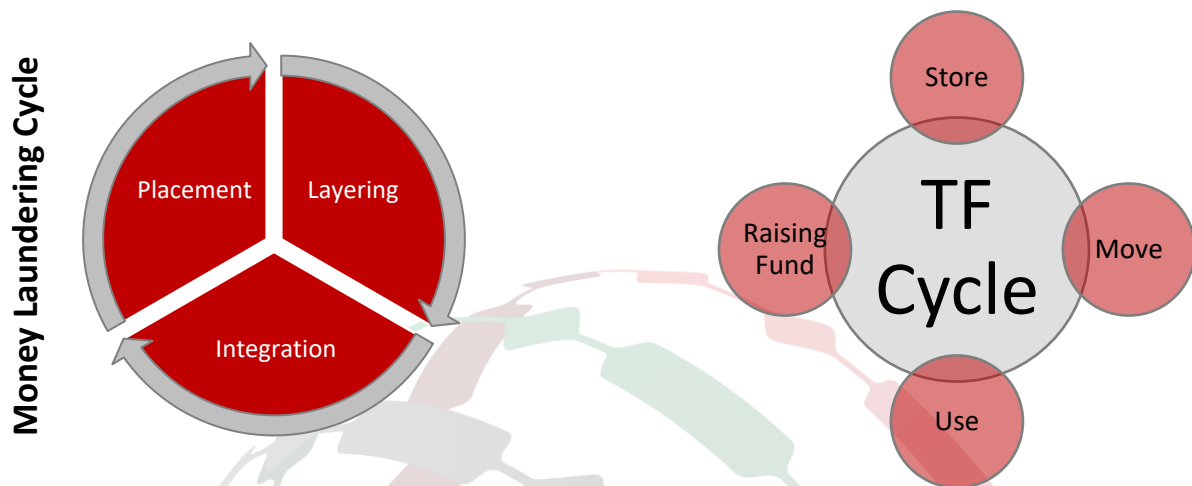


CHART 1: *ML cycle vs. TF cycle*

A noteworthy piece of academic work (Davis, 2021) has consolidated the above four stages to consider two additional classifications: management of funds (which entails the managing of raised funds through, for example, investment and schemes used to generate the organization’s profit), and obscuring of funds (describing tactics used to hide the funds).²⁹

5. OVERVIEW OF GLOBAL TERRORIST FINANCING TYPOLOGIES

Terrorists’ expenses and sources of income depend on their organizational structure and location. Therefore, terrorists’ required funds may vary from one group to another; however, the methods and techniques that they use to collect and move their money are almost identical.

Sources of terrorists’ funds could be explained in the following typologies:

1. **Crowdfunding and donations:** Despite its economic purpose being to finance legitimate businesses, crowdfunding has always been an attractive method for terrorist and extremist groups in raising their funds, due to its ease of use and swift accessibility worldwide.³⁰ Crowdfunding entails both physical and digital fundraising through payment processing service providers, Fintech³¹ platforms, social media, and other digital platforms. Payment can be

²⁹ Davis, J. (2021) *Illicit Money: Financing Terrorism in the 21st Century*. Colorado: Lynne Rienner Publishers. The introduced additional classification was found to be more consistent with the data used in this report.

³⁰ FATF (2023) *Crowdfunding for Terrorism Financing*. Available at: <http://www.fatf-gafi.org/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html>; and FATF (2021) *Ethnically or Racially Motivated Terrorism Financing*. Available at: <https://www.fatf-gafi.org/publications/methodsandtrends/documents/ethnically-racially-motivatedterrorism-financing.html>

³¹ Fintech refers to the term Financial Technology, which describes “mobile applications, software and other technology that enable users and enterprises to access and manage their finances digitally” (IBM, no date).

collected in different forms, through cash, wire transfers and remittances, or virtual currencies. This process often involves multiple intermediaries and third parties, while contributors can be knowingly or unknowingly involved in TF activities, and/or the abuse of non-profit organizations (NPOs).³² Within this context, the UNSC underlined, in its resolution 2462 (2019), the concern regarding terrorists and their supporters using information and communications technologies in crowdfunding to fund their terrorist acts.

Within the same context of crowdfunding, the NPOs sector is vulnerable to terrorists' abuse (in both raising and moving funds) aimed at financing those terrorists' organizational needs and activities through their adherents' donations and support.³³ NPOs play a significant role in states' social systems and economy by providing essential support and aid to those in need. Governments facilitate the establishment of these organizations and reduce their cost of business through fewer constraints in their operations and tax exemptions.³⁴ Nevertheless, terrorist groups have been known to abuse the NPOs in different forms, including the diversion of funds to their own accounts, affiliations with terrorist entities, facilitating recruitment on behalf of terrorist groups, abusing and manipulating programs intended for the public, and false representation through sham NPOs.³⁵

2. **Extorting territories under terrorists' control:** Terrorists take advantage of the resources available in territories under their control to generate their funds. For example, in Syria and Iraq, the Islamic State of Iraq and the Levant (ISIL) generated revenue from citizens under the names of 'Zakat,' 'charitable giving,' and 'taxation.'³⁶ The aforementioned are in addition to illicit trading in natural resources and looting activities.
3. **Self-funding from criminal proceeds:** Terrorist groups have been involved in criminal acts to generate the funds required for their activities since the 1970s, as an alternative to state sponsorship of terrorism.³⁷ Illicit funds are recognized as being generated through different crimes, such as drug trafficking, fraud, robbery, and illicit trade in various products, e.g. smuggling cigarettes, ivory, charcoal, contraband sugar, and counterfeit products.³⁸ The said examples underline how TF and ML are similar in terms of their involvement of criminal acts.

³² Ibid

³³ FATF (2023) BPP-Combating the Terrorist Financing Abuse of Non-Profit Organisation. Available at: www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html

³⁴ Bolleyer, N. and Gauja, A. (2017) 'Combating terrorism by constraining charities? Charity and counter-terrorism legislation before and after 9/11', Public Administration. Available at: <https://doi.org/10.1111/padm.12322>

³⁵ ManchesterCF-FIU Connect: Terrorist Financing.

³⁶ FATF (2015) Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL).

³⁷ Ryder, N. (2015).

³⁸ FATF-GAFI (2008); and FATF (2015) Emerging terrorist financing risk.

4. Self-funding from legitimate sources: Self-funding could be generated from the salaries of the terrorists themselves or their families' wealth, especially when the amount of money needed for the operations is low.³⁹ However, given their needs, terrorist organizations may engage in legal business to generate their own funds, including establishing front companies and misusing the trade system to facilitate fund transfers as well as to conceal the origins of their money. Front companies can also be used to deceive authorities by providing fabricated documents such as overestimated prices, double invoices or sham transactions.⁴⁰ Since 2001, several official reports and research articles have highlighted how terrorists' business varies, including trading in various companies, hospitality, restaurant chains, and ventures in real estate and stocks.⁴¹ The examples introduced here highlight how TF is different from ML, as, with the former, the origin of the terrorists' funds is legitimate, which might challenge competent authorities and the financial sector practitioners when it comes to tracing terrorists' funds.

6. EMERGING TYPOLOGIES AND UTILIZATION OF SOPHISTICATED TECHNOLOGIES

The UNSC CTED (2024) reported on the evolving trends in financing foreign terrorist fighter (FTF) activity, mainly linked to ISIL-inspired FTFs, stating that TF methods continue to involve donations from terrorist supporters abroad, in addition to self-financing their travel to zones with terrorist activities. Nevertheless, adaptability to sophisticated technologies and obfuscation techniques is also acknowledged, including collecting funds through encrypted mobile applications and utilizing virtual assets mixed with traditional methods such as Hawala and cash couriers.⁴²

Moreover, there are some examples of supporters of terrorism and extremists using Artificial Intelligence (AI), Large Language Models (LLMs), and deepfake in their propaganda material (EUROPOL, 2024). Employment of sophisticated technologies in TF techniques, whether through modern financial services and payment platforms, online crowdfunding and social media sites, or virtual assets, in particular, has been recognized as a growing concern globally over the past few years.⁴³ Different studies have shown that Fintech-offered services and social media domains⁴⁴

³⁹ FATF-GAFI (2008).

⁴⁰ Acharya, A. (2009).

⁴¹ E.g., FATF (2015) Emerging terrorist financing risk; and Kaplan, D., Fang, B. and Sangwan, S. (2005) 'Paying for Terror', U.S. News & World Report, 139 (21), 40–54. Available at:

<http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=18954932&site=ehost-live>

⁴² CTED (2024) CTED Trends Tracker.

⁴³ United Nations Security Council – CTED (2022) Technical sessions: Threats and opportunities related to new payment technologies and fundraising methods. Available at: <https://www.un.org/securitycouncil/ctc/ru/node/39098>; EGMONT Group (2023) Report on Abuse of Virtual Assets for Terrorist Financing Purposes. Available at: <https://egmontgroup.org/news/public-summary-on-abuse-of-virtual-assets-for-terrorist-financing-purposes-report/>; and FATF (2023) Crowdfunding for Terrorism Financing.

⁴⁴ Social media domains include: social networking services, content hosting services, crowdfunding services, and internet communication services. APG/MENAFATF (2019) Social Media & Terrorism Financing Report. Available at: <https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142>

were observed in different TF cases. Nevertheless, their extent remains limited in comparison to conventional financial methods.⁴⁵

Different publications and research have pointed out that terrorist individuals and groups have been shifting from traditional finance and scaling up their usage of cryptocurrency to transfer funds for operational purposes (e.g., Chainalysis, Elliptic, and TRM Labs). Based on Chainalysis' (2025) aggregation of crypto flows for the benefit of 'extremist groups'⁴⁶ across different regions during the period spanning 2012–2024, the average transaction amount remained in the hundreds of dollars each year, with the exception of 2022 during COVID-19.⁴⁷ According to TRM (2025), ISIL (ISKP in particular)⁴⁸ is growing its use of cryptocurrency in planned terrorist acts, with identified transactions ranging from USD100 to USD15,000 processed through regulated virtual asset service providers (VASPs) and other crypto traders.⁴⁹ Similarly, Chainalysis broke down different Bitcoin transactions, showing its use in donation campaigns for Al-Qaeda, along with several related terrorist groups.⁵⁰

Therefore, different data has shown that the use—by terrorists and extremist individuals and groups—of cryptocurrency in raising funds is escalating, through Bitcoin as well as other types of privacy coins, in addition to encrypted chat rooms and social media. Nevertheless, it is deemed that traditional finance and stablecoins remain the primary choice for terrorist groups' financing.⁵¹ Therefore, the utilization of cryptocurrency by terrorist organizations is perceived to make up only a small share of cryptocurrency-related illicit transactions.⁵²

7. OVERVIEW OF TF NATIONAL RISKS AND LEGAL FRAMEWORK

The terrorist financing offence is defined in Article 29 of the UAE Federal Law No. 7 of 2014 on "Combating Terrorism Crimes" as **Whoever**:

Offers, collects, prepares, obtains or facilitates the obtainment of funds for the purpose of using same although aware that they will be used, in part or in whole, in the commission of a terrorist offence;

⁴⁵ RUSI (2022) Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks – Project Craaft. Available at: <https://www.rusi.org/explore-our-research/publications/occasional-papers/bit-bit-impacts-new-technologies-terrorism-financing-risks>

⁴⁶ According to Chainalysis methodology, the term extremist groups is used to describe "organizations or financial activities involving groups across the political and ideological gamut that may still not meet the criteria for designation as Foreign Terrorist Organizations (FTOs) in the United States".

⁴⁷ Chainalysis (2025) Crypto Crime Report. Available at: <https://go.chainalysis.com/2025-Crypto-Crime-Report.html>

⁴⁸ Islamic State – Khorasan Province (ISKP) is a branch of the Islamic State active in Central and South Asia (primarily Afghanistan, Pakistan, Tajikistan and Uzbekistan). More information available at: <https://www.csis.org/blogs/examining-extremism/examining-extremism-islamic-state-khorasan-province-iskp>; <https://www.washingtoninstitute.org/policy-analysis/islamic-states-external-operations-are-more-just-iskp>

⁴⁹ TRM (2025) Crypto Crime Report. Available at: <https://www.trmlabs.com/resources/reports/2025-crypto-crime-report>

⁵⁰ Chainalysis Intelligence Brief (2020).

⁵¹ TRM (2025) and EUROPOL (2024).

⁵² Chainalysis (2024) Assessing Terrorism Financing On-chain is Crucial and Complex. Available at: <https://www.chainalysis.com/blog/assessing-terrorism-financing-on-chain/>; Elliptic (2024) Typologies Report. Available at: <https://www.elliptic.co/resources/elliptic-typologies-report-2024>

Offers funds to a terrorist organisation or person or collects, prepares, obtains or facilitates the obtainment of funds for such terrorist organisation or person, although aware of their purpose;

Acquires, takes, manages, invests, possess, transmits, transfers, deposits, keeps, uses or disposes of funds or carries out any commercial or financial bank transaction although aware that all or part of such funds are collected as a result of a terrorist offence, owned by a terrorist organisation or intended for the financing of a terrorist organisation, person or offence;

Is aware that the funds are, in whole or in part, collected as a result of a terrorist offence, owned by a terrorist organisation, illegal, owned by a terrorist person or intended for the financing of a terrorist organisation, person or offence.

TF offences are punished by life or provisional imprisonment for a term not less than ten years, and a fine not less than three hundred thousand (300,000) AED and not exceeding ten million (10,000,000) AED shall be imposed on anyone who uses the proceeds in financing terrorism (Federal Law No. 7 of 2014: Articles 29-30; Federal Law No. 20 of 2018: Article 22).⁵³ These are in addition to other provisions on legal persons convicted in financing terrorism or financing illegal organizations, including liquidations and suspension of the office where the legal person practices its activity (Article 23). In the event of proving the committing of a crime, confiscation shall be made whether the funds, proceeds, instrumentalities are in the possession or ownership of the perpetrator or another party, without prejudice to the rights of bona fide third parties (Federal Law No. 20 of 2018: Article 26). As regards breaching the directives of the UN Security Council concerning the financing of terrorism and the proliferation of weapons of mass destruction, imprisonment (no less than one year and no more than seven) and a fine of no less than AED50,000 and no more than AED5,000,000 are applied (Article 28).

According to the UAE's TF National Risk Assessment (NRA) in 2024, TF activities pose a medium-high risk in the UAE. The assessment underlined TF methods, including donations (sent abroad) and the role of the informal financial networks, the use of unregulated money service providers, and manipulation of the trade sector. The vulnerabilities of legal persons, the shipping sector, MSBs, and Hawala service providers were assessed and deemed significant. The said conclusion from the NRA is consistent with the findings of this report.

8. ANALYSIS OF TF-RELATED STRS/SARS

The UAEFIU conducted comprehensive strategic analysis of all received TF-related STRs/SARs from **01/01/2021 to 31/12/2024**, based on the Reason for Reporting (RFR) selected by the reporting entity upon submission to the reporting system. Overall, **397 reports** were filed by reporting

⁵³ Federal Law No. 7 of 2014. Available at: <https://uaelegislation.gov.ae/en/legislations/1018> ; Federal Law No. 20 of 2018. Available at <https://uaelegislation.gov.ae/en/legislations/1016> and its amendment by Federal Law No. (26) of 2021.

entities, related to possible TF during the examined four-year period. Year-to-year analysis has shown an increasing pattern, as illustrated in **Chart 2**. However, evaluation of these suspicious reports' quality, including validity and reliability, concluded that only **199 STRs/SARs** (100 STRs and 99 SARs), **representing 50%** of the said 397 reports, met the evaluation criteria to construct reasonable grounds for TF concern.

Examples of the most common reasons for classifying the remaining invalid STRs/SARs include the following, with no particular order:

- Selecting wrong reason for reporting.
- Suspicion was reported based on the subject's nationality solely.
- Missing customer identification details (whether in text or attachment).
- Missing attachments or supporting documents to establish the TF suspicion (e.g., reporting subjects as listed/sanctioned terrorists based on adverse media with no supporting documents while the UAEFIU screening on the subjects and search of open-source data found no similar concern).
- Absence of TF indicators rather than money laundering or other crimes concern.

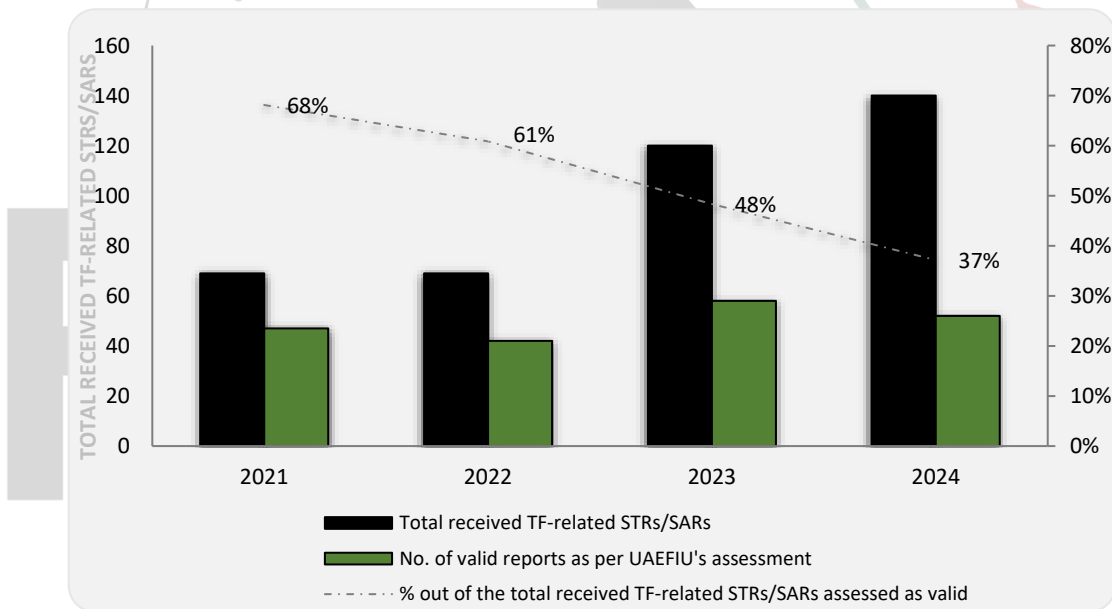


CHART 2: Overview of received TF-related STRs/SARs from 2021 to 2024

Based on the main concern(s) chosen by reporting entities during their submission of STRs/SARs to the reporting system, **Chart 3** illustrates the ten most frequently used RFRs.

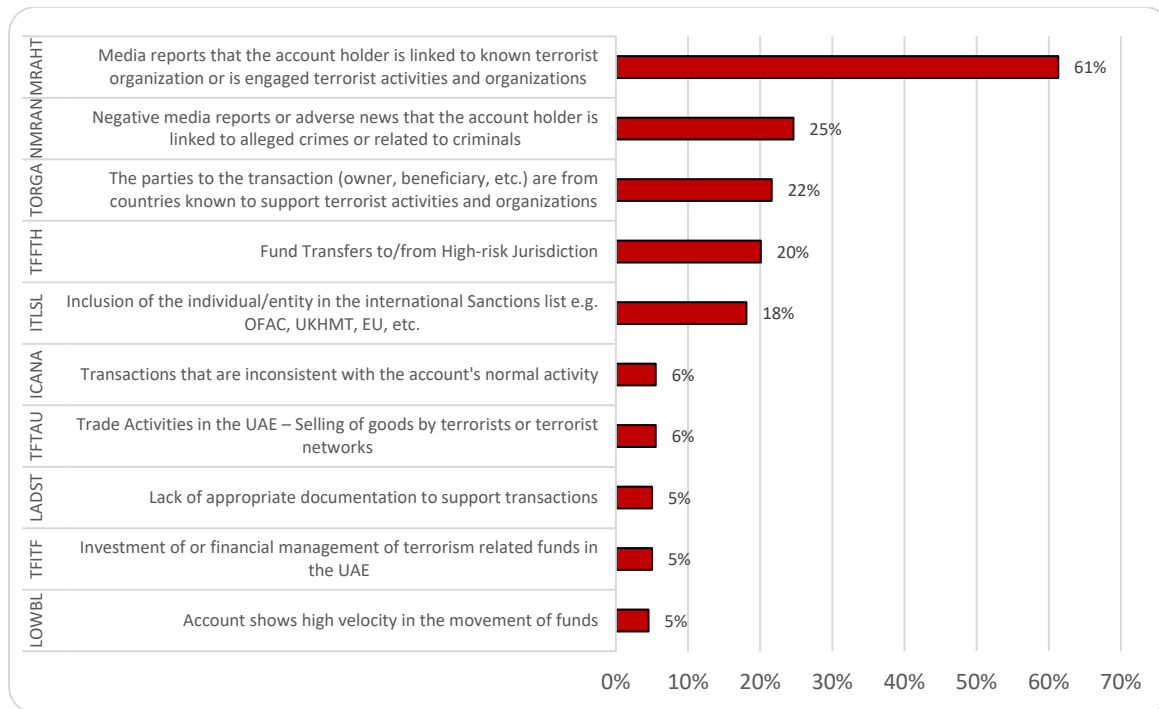


CHART 3: Top 10 Reasons for Reporting (RFRs)

9. IDENTIFIED TF TYPOLOGIES AND TRANSACTIONAL PATTERNS

The following section provides a brief overview of the identified TF typologies suggesting sectors' vulnerability:

9.1. Movement and obscuring of funds through financial institutions

As highlighted by the FATF (2015), the banking sector is vulnerable to TF, since terrorists often misuse the sector's international wide reach and swiftness in moving their funds.⁵⁴ Similarly, MSBs and the remittance sector are also misused in moving terrorists' illicit funds.⁵⁵

The majority of the reviewed data underlined the use of third parties or intermediaries in facilitating the movement of funds through financial institutions while the ultimate beneficiaries remained unidentified.

9.2. Movement of funds through unlicensed Hawala

It is globally recognized that restricting the formal financial system typically leads to the use of unregulated money service providers/Hawala, and there have been many published examples of

⁵⁴ FATF (2015) Emerging Terrorist Financing Risks.

⁵⁵ FATF-GAFI (2008) Terrorist financing report.

terrorists using Hawala and other service providers to transfer their funds.⁵⁶ The examined data indicated in this report showed the possible use of unlicensed Hawala.

9.3. Establishment of corporate networks to move and obscure terrorist funds

The most frequently observed pattern in the analyzed STRs/SARs and TF-related cases emphasized the role of corporate structure being abused by terrorist groups. This pattern is mostly employed by third parties and nominees on behalf of terrorist groups or adherents, who would facilitate the establishment of a network of companies across different regions to enable the layering and transfer of funds across the network.

9.4. Movement of Funds through trade-based terrorist financing (TBTF)

Trade-based terrorist financing (TBTF) techniques were observed in several scenarios illustrated in the examined data, specifically through the establishment of a network of shell entities to trade in different items inconsistent with the licensed business activity and trade documents. Transactions would ultimately benefit a listed terrorist group locally or internationally.

9.5. Trading in high-value items and goods to generate funds

As globally recognized and explained earlier in this report, different terrorist organizations self-fund through resources within their area of control or in high-value goods. Data utilized in this analysis illustrated different scenarios within this context.

9.6. Misuse of the real estate sector

A frequent pattern observed in the data suggested suspicious transactions ultimately directed toward the real estate sector.

9.7. The misuse of virtual assets in crowdfunding and movement of funds

Data implied different indications relevant to suspected individuals linked to terrorist individuals/networks or high-risk jurisdictions of conflict. Observed scenarios included suspicions of cryptocurrency address/wallet (owned by a subject of STR/SAR) being controlled by a

⁵⁶E.g., FATF (2013) The Role of Hawala and other similar service providers in money laundering and terrorist financing.

designated terrorist individual/group or used to transfer the funds in the form of digital currency among the network/counterparties.

9.8. Crowdfunding through local accounts and foreign NPOs

Data utilized in this analysis showed no valid indications on the abuse of local NPOs in TF activities. However, some suspicious reports implied the involvement of foreign NPOs, potentially as a source of TF funds or to gain access to the international financial system. Local legal persons would be funded by different foreign NPOs in addition to multiple foreign legal persons across different regions under the claim of trade. Subjects from the UAE were suspected of being used as pass-through accounts to move the funds across different destinations.

9.9. Movement and obscuring of funds through settlement of loans

Few STRs underlined the claim of loans settlement among a network of legal persons (local and foreign) in transactions involving individuals/family members of individuals designated in relation to TF.

9.10. Movement of funds through high-risk jurisdiction or neighbors

Transactions reviewed within the context of this report frequently involved countries with lax AML/CTF regimes or those known for terrorism/TF activities or neighbors to the latter. The UAE financial sector would be used as a pass-through account/hub originating from/directed to those jurisdictions.

9.11. Potential illicit funds and other financial crimes as source of funds

The analyzed data illustrated several misconducts and criminal proceeds suspected to be involved in financing terrorist networks and individuals or correlated with being sanctioned or placed on TF-related lists (be it foreign or national). These crimes did not necessarily take place in the UAE, and were rather observed being used in the network schemes across different jurisdictions, notably: drug trafficking, kleptocracy, bribery, fraud, smuggling of cash and high-value items (e.g., antiquities, gold, diamond, fuel, etc.), arms trafficking, production of illegal weaponry, conspiracy, cybercrime, and unlicensed Hawala activities or black-market currency exchange abroad.

Moreover, different examined scenarios implied the employment of middlemen between organized criminal networks and the involved terrorist groups to facilitate the groups' operational materials and arms trafficking.

10. ROLE OF TF FACILITATORS AND INTERMEDIARIES

10.1. Designated and listed individuals and entities

Many of the examined suspicious reports and cases were reported in relation to a designated individual, entity, or a terrorist group, whether internationally, nationally, or by other foreign regulators.

10.2. Political extremists and high-risk jurisdictions of terrorism

The data suggested connections to political extremists or corrupt officials, thus enabling access to resources, influence, or facilitating TF activities in conflict zones or comprehensively sanctioned jurisdictions. Different scenarios implied the involvement of foreign PEPs in financial crime in general and TF in specific to support political parties/influential figures with similar ideologies designated by national or foreign sanction regimes as terrorist groups.

10.3. Family members

The role of family members, including the spouses/siblings of sanctioned individuals in relation to terrorism/TF who are residing in the UAE were observed in different scenarios. The most notable occurrences were the establishment of legal persons and offshore entities and the purchasing of real estate in the UAE.

10.4. Money mules

Analysis of suspicious reports revealed the employment of low-income earners' (blue-collar) and mules' accounts to conduct small frequent transactions below the threshold. A group of foreign nationals in the UAE would be recruited to receive different amounts of funds from abroad, where the controller might be present.

10.5. Corporate nominees

Many of the examined scenarios underlined the role of subject nominees or strawmen/women, i.e., administrative individuals with no previous business experience from specific foreign countries assigned as owner/shareholder/manager to conceal the actual identity of the beneficial owner who, in most cases, was found to be sanctioned in relation to financing/facilitating the financing of terrorist groups.

10.6. Lawyer, accountants, and corporate service providers

A number of suspicious reports illustrated the role of foreign accountants and lawyers abroad in orchestrating money laundering and TF activities or serving as intermediaries in facilitating transactions and possibly providing legal/financial cover for illicit activities.

11. DEVELOPED RISK INDICATORS

The UAEFIU developed a list of risk indicators based on the analyzed data, including suspected transactions and observed TF scenarios. These risks indicators aim to guide the UAEFIU's stakeholders in detecting unusual transactions and behaviors relevant to TF, as well as transaction monitoring. It is worth recalling that criminal activity cannot explicitly be concluded based on a single indicator, but rather a combination of these indicators, in order to ascertain such suspicion. The following risk indicators should also be considered together with FATF-identified red flags in relevant publications and sources referenced in this report.

Customer's characteristics and associates

1. An account owner's name or counterparty is listed on a terrorist list (foreign or local).
2. A customer who is identified as a family member or relative to a designated person due to terrorism/TF concerns.
3. Politically Exposed Persons (PEPs) with links to conflict zones or extremist groups.
4. Customer associations with entities suspected of trading in conflict gold or individuals from high-risk jurisdictions linked to gold smuggling in conflict zones.
5. A customer is dealing with a counterparty who is a subject of a previously filed STR/SAR concerning possible TF activities.
6. A customer is dealing with a counterparty who is the subject of adverse news concerning possible TF activities.
7. Customer's counterparties are reported or observed to have similar suspicions in relation to terrorism or TF.

Behavioral patterns

8. Changes in transactional pattern once a counterparty to the customer has been listed by a sanction regime due to terrorism/TF concerns.
9. Multiple entity accounts owned or managed by a customer who has dual nationality or more (one of them from a country known for high terrorism activities/being the home of terrorist groups) and which show transactions that are not declared at the time of onboarding or are different from the declared line of business.

10. A customer is sending/receiving multiple transfers involving unknown sources of funds or where there is no clear relation between the senders and receivers from/in high-risk jurisdictions, under the purpose described as “family assistance” or “gift.”
11. An account opened by a non-resident, or remittance transaction by a non-resident involving high-risk jurisdictions known for terrorism or conflict zones.
12. The account observes several remittances from/to different territories, including conflict zones or territories that embrace terrorist groups and activities.
13. Customers declare, to their financial institution, that they intend to travel or have previously travelled to regions known as being conflict zones.
14. A beneficial owner of a local legal person classified as PEP and representing a political party in a high-risk jurisdiction known for terrorism or neighboring destabilized territories.
15. A foreign PEP from a country with a high risk of terrorism or which is the home of terrorist groups, seemingly intended to undeclare his/her status during onboarding with the reporting entity.
16. A concern on the customer’s personal documents, including a suspicion of using falsified or fabricated identity documentation to establish multiple legal persons and then using their accounts to transact with undeclared counterparties overseas.
17. A customer name written in different forms or holding more than one nationality and various residential addresses and phone numbers.

Transactional patterns

18. Frequent wire transfers to countries or neighbor countries known for terrorism activities/being the home of terrorist groups.
19. A personal account receiving a salary from an entity (local or foreign) listed/owned by sanctioned individual in relation to terrorism/TF.
20. Transactions showing customer’s frequent travel (customer’s transaction locations, such as ticket and hotel booking, transactions relevant to groceries, restaurants and shops, etc.) involving countries or neighbor countries known for having high levels of terrorism.
21. A personal account owned by a national of a high-risk country witnessing a high volume/value of transactions toward global (online) auction websites known for trading in arts and high-value items or art galleries abroad.
22. A bank account witnessing deposits from multiple parties, followed by withdrawals abroad in/close to a high-risk jurisdiction known for terrorism activities.
23. Multiple remittances (through MSBs) of small amounts by the same person or a group of individuals having the same nationality sent to a high-risk jurisdiction known for terrorism activities/being the home of terrorist groups, or a neighboring jurisdiction.

24. The frequent changing of currency of high demand or value by an individual or a group of individuals of the same nationality who are known, to the reporting entity, for being of high-risk.
25. Transactions involving foreign currency exchanges that are followed, within a short time, by remittances to high-risk locations.
26. High volume of transactions by multiple individuals having more than one nationality, including the nationality of a country known for terrorism activities or conflict zones.
27. A legal person owns shares in (or transacts with) another legal person with historical links to a terrorist group or supports the activities of a political party in conflict zones.
28. High volume of transactions by a business account engaging with other counterparties that are not in line with the customer's licensed business activities, and/or are located near to conflict zones.
29. Significant movement of funds through local legal entities transacting with holding companies in high-risk jurisdictions known for a lax AML/CTF regime or jurisdictions known for terrorism/being the home of terrorist groups.

Transactions involving shipping and cargo

30. Complex route of shipments involving jurisdictions known for having a high risk of terrorism or a weak AML/CTF framework.
31. Unusually high amounts of remittances sent through MSBs (or banks) as salaries to vessels' crew/logistics and shipment agents where shipments' activities are/suspected of being linked to jurisdictions known for high corruption/terrorism activities or sanctioned entities.
32. Inconsistent information in trade documents, especially bill of lading where the destination/origin (of high-risk jurisdiction) of shipments is suspected of having been altered, or trade documents are not provided by the customer.
33. Movement of shipment(s) cannot be validated, or lack of transparency in the overall trade (e.g., non-submission of trade documents such as delivery order, certificate of origin, bill of lading/airway bill, importation and exportation bill issued by customs of the respective country of destination) while trading in high-value commodities.
34. Open-source data showing that a freight carrier used by the customer has links to terrorist groups.

Transactions of crowdfunding and fundraising

35. Funds being received from parties found to be subjects of negative media/open-source data for being connected to terrorist groups' charities.
36. A customer is sending/receiving frequent money to/from a foundation/charity that is not in line with the customer's business profile.

37. Dealing with a foreign NPO that has no public presence and is operating in jurisdictions with a high level of terrorism.
38. Foreign NPOs transacting with a customer licensed for retail business or other different lines of business with no logical economic purpose.
39. Funds sent from foreign NPOs located in a high-risk country to local entities to then be retransferred to other entities abroad in different regions, or entities located in/close to conflict zones.
40. The raising of donations by a legal person without being properly licensed or registered by the Ministry of Community Development for opening accounts to collect donations.
41. A NPO uses an unnecessarily complex pattern of transactions or layering among a network of legal persons for its operations overseas.
42. Account holder receiving an unusual volume of funds from unknown sources who has been found, through open-source data, to have social media accounts used to raise donations or advertise content describing extremists' ideology.
43. Use of internet platforms and social media channels (e.g., Telegram) to organize deposits and withdrawals using the customer personal or corporate account linked to (or a sympathizer of) a designated terrorist individual or group.
44. Account holder receiving an unusual volume of funds from unknown sources who has been found, through open-source data, to have links to, or followers known to be sympathetic toward, extremists' ideology or designated terrorist individuals or groups.

Transactions involving real estate

45. Real estate business account is witnessing a high volume of transactions from/to multiple natural and legal persons in different countries known to have a high risk of terrorism/TF activities or linked to TF-sanctioned individuals/entities.
46. Purchase and sale of real estate in a short period of time followed by immediate purchase of another piece of real estate in full payment involving non-resident customers from high-risk jurisdictions known for terrorism or neighboring a jurisdiction of terrorism activities.

Transactions involving high-value items

47. A business account conducts a high volume of transactions periodically in specific commodities that are not in line with the customer's business. These commodities could be traded for cash or shipped to areas of conflict (e.g., used or new cars).
48. A customer (owner, authorizer of the account, etc.) from countries known to support terrorist activities and organizations conducting trade activities in gold or transactions with trade parties located in areas of conflict known for illegal mining/conflict gold.

49. A personal account receiving a high value of fund(s) as a salary from non-financial businesses and professions (e.g., accountant, lawyer) abroad, while the customer is known to the reporting entity to be an owner of a high-value industry business (e.g., gold, diamonds, oil, electronics).
50. Multiple companies trading in precious metals and stones owned by the same owner/frequent owners from a country known for being home to an identified terrorist group.

Transactions involving Cryptocurrency

51. Customer's private crypto wallet interacts directly/indirectly with a trading platform sanctioned by a regulatory authority due to its link to a high-risk jurisdiction.
52. A customer's crypto wallet address appears on jihadist or extremist-sponsored social media or fundraising sites.
53. Transfers to/from wallets linked to individuals or exchanges located in high-risk TF jurisdictions.

Secondary risk indicators

The following secondary risk indicators have been identified in some TF-related scenarios. These secondary indicators might also appear in other illicit activities (money laundering and other financial crimes), and hence they might be recognized within the context of TF after previously identified primary indicators are detected.

1. High volume of funds seemingly being re-routed to a family member followed by immediate transfer to an overseas account without a logical justification.
2. Deposits of a high volume of cash with an unexplained origin or incomplete documentation (i.e., bank statements, cash declarations from customs).
3. Significant cash deposits through ATM/CCDM and inward remittance below the threshold, followed by online international and local money transfers.
4. Both savings and current account are used in addition to excessive credit cards being obtained by the same person.
5. Remitting funds through different MSBs in a structured manner within a short period of time without proper justification.
6. Multiple companies opened by the same person/relatives at the same registrar within the same period on sequential dates.
7. The account activities show intense inward transfers from different legal entities followed by cross-border remittances to other entities in the same line of business, but no operational expenses are observed in the account to validate the commercial activity.

8. Corporate account receiving different transfers in foreign currency from several counterparties located in different countries, to be shortly transferred to other local counterparties in AED currency.
9. Rounded transactions among counterparties with different lines of business (including companies trading in oil and petrochemicals, machinery and spare parts, electronics, precious metals and stones, and real estate brokerage or development and construction).
10. A company established with low capital receiving a high volume of transfers and cheque deposits once its account has been opened, followed by immediate withdrawal through transfers and cheques toward other counterparties in different lines of business.
11. A foreign resident owns multiple high-profile companies with no previous business experience.
12. Suspicion of a customer's behavior in deliberately avoiding thresholds to evade detection.
13. Multiple changes in the corporate structure, including entity name, beneficial owner percentage/shareholders, managers, and line of business, or a sudden change in the nationality of one of the UBOs.
14. Multiple legal persons established sequentially at the same time, at the same location, co-owned and/or managed by the same individual or sharing the same address.
15. A beneficial owner of a local entity found to be the same beneficial owner of a foreign entity that has been frequently transacting with the local entity's account.
16. A customer who has an excessive number of accounts in different currencies at the same financial institution or within different institutions, using them with his/her corporate accounts in receiving/sending funds locally and internationally.
17. Multiple personal accounts opened by the same person—who works in a low- to medium-income or administrative job—being used in receiving a high volume of deposits and/or wire transfers.
18. A natural person opening an account solely for the purpose of receiving transfers, to be immediately followed by a withdrawal.
19. Multiple legal entities connected by the same owner or counterparties with no apparent business transactions showing routing/transitory behavior under the purpose "Goods Bought or Sold."
20. A large inward remittance/wire transfer from a foreign shipping company, with supported invoices different from the business activities and/or not aligning with providing shipping services.
21. A customer providing a bill of lading with no reference or container number and rejecting providing the original documents or further supporting documents.
22. Transactions showing multiple counterparties relevant to shipping/customs clearance with no supporting shipping/trading documents.
23. Buying and selling properties through offshore networks to move illicit funds.

24. The use of virtual assets to send funds to a few selected wallets that can be traced to unregulated or non-compliant virtual asset service providers.
25. Customer attempts to establish accounts with false identity documentation or purchase cryptocurrency with a third-party card.
26. A non-cooperative customer who is not responding when asked to provide the delivery and shipment documents for the transaction or any other documentary evidence requested by the reporting entity.
27. Unwillingness of the customer to cooperate and provide clarifications on the transactions of concern.
28. No valid economic and commercial purpose has been established for the transaction.
29. Ultimate source of funds and utilization cannot be ascertained.
30. Transactions that are inconsistent with the account's normal activity.
31. Lack of appropriate documents to support transactions.
32. Account shows high velocity in the movement of funds.

12. CONCLUSION

The UAEFIU's strategic analysis followed a designed methodological approach in data collection and analysis that fits with the TF nature and cycle of fund, as well as the nature of data obtained or available within the UAEFIU databases. The analysis outcome has offered an understanding of global identified TF typologies and how they are linked to local recognized TF patterns.

The UAEFIU has identified different risk indicators which are directly or indirectly relevant to TF. Reporting entities are urged to consider these indicators in detecting or investigating TF-related incidents. Upon applying these risk indicators, reporting entities should not refer to only one indicator to determine whether a transaction is suspicious or linked to a terrorist activity. Risk indicators indicated in this report are not exhaustive nor exclusive.

Reporting entities should consider multiple risk indicators in addition to other factors relevant to their customer's characteristics, including customer risk profile and overall financial activities during the established relationship period with their customers. These are in addition to open sources and screening tool available to the reporting entity.

Overall, reporting entities should ensure reported information quality, including its accuracy and relevancy to terrorism or TF concern, correctness, and completeness, and provide all documents supporting the established suspicion. Moreover, reporting entities should consider providing dedicated training on detection and investigating TF related activities and transactions.