



مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Notice No. : CBUAE/BSN/N/2021/5737

Date : 16 December 2021

Class. : Restricted

To : All Financial Institutions operating in the UAE

Subject : Updated Guidance on Targeted Financial Sanctions and Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction

إشعار رقم : CBUAE/BSN/N/2021/5737

التاريخ : 16 ديسمبر 2021

التصنيف : محظور

إلى : كافة المؤسسات المالية العاملة في الدولة

الموضوع : إرشادات بشأن العقوبات المالية المستهدفة وأنماط الالتفاف على العقوبات المستهدفة المرتبطة بالإرهاب وتمويل الإرهاب وانتشار أسلحة الدمار الشامل

After greetings,

بعد التحية،

We refer to our Notice No. 2893/2021 dated 02/06/2021, regarding (a) "Guidance on Targeted Financial Sanctions for Financial Institutions and Designated Non-Financial Business and Professions (DNFBPs)" and (b) "Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction".

بالإشارة إلى إشعارنا رقم 2893/2021 المؤرخ 02/06/2021، بشأن (أ) "دليل إرشادي بشأن العقوبات المالية المستهدفة للمؤسسات المالية والأعمال والمهن غير المالية المحددة" و(ب) "أنماط الالتفاف على العقوبات المستهدفة المرتبطة بالإرهاب وتمويل الإرهاب وانتشار أسلحة الدمار الشامل".

Please find attached updated versions of the above-mentioned documents and associated TFS Private Sector Mini Guide issued by the Executive Office of the Committee for Goods and Material Subjected to Import and Export Control.

تجدون مرفق الإصدارات المحدثة للوثائق المذكورة أعلاه والدليل المبسط عن العقوبات المالية المستهدفة للقطاع الخاص ذات الصلة والصادرة من قبل المكتب التنفيذي للجنة السلع الخاضعة لرقابة الاستيراد والتصدير.

Financial Institutions should consult the Central Bank's and the Executive Office's websites respectively as updated from time to time.

يجب على المؤسسات المالية الاطلاع على التحديثات التي تتم على المواقع الإلكترونية للمصرف المركزي والمكتب التنفيذي من وقت لآخر.

<https://www.centralbank.ae/en/cbuae-amlcft>

<https://www.uaieec.gov.ae/en-us/un-page#>



مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

You are required to circulate the mentioned documents to all your branches electronically. يجب عليكم تعميم المستندات المذكورة على كافة فروعكم إلكترونياً.

Yours faithfully,

وتفضلوا بقبول فائق الاحترام،

أحمد سعيد القمزي
مساعد المحافظ – الرقابة على البنوك والتأمين

Ahmed Saeed Al Qamzi

Assistant Governor for Banking and Insurance Supervision

Encl.

مرفقات:

Guidance on Targeted Financial Sanctions

For Financial Institutions (FIs), Designated Non-Financial Business and Professions (DNFBPs) and Virtual Assets Service Providers (VASPs).

Issued by the Executive Office of the Committee for Goods Subject to Import and Export Control

© Executive Office of the Committee for Goods Subject to Important and Export Control, 2021

BurDubai - Umm Hurair
1 - Khalid Bin Al Walid St
Consulates Area in the Ministry of Foreign Affairs and International Cooperation / Dubai Office

<https://www.uaieiec.gov.ae/en-us/>

Telephone: +971 44 040 040

Fax: +971 43574499

Email: iec@uaieiec.gov.ae

Issued on: 14 Jan 2021

Last amended: 14 Nov 2021

Acronyms

DNFBPs	Designated non-financial businesses and professions
Executive Office or EO	The Executive Office of the Committee for Goods & Material Subjected to Import & Export Control
FATF	Financial Action Task Force
FIs	Financial Institutions
FIU	Financial Intelligence Unit
Local Terrorist List	National terrorist list issued by the UAE Cabinet
MOFAIC	Ministry of Foreign Affairs and International Cooperation
Other Measures	Other sanctions measures besides freezing. These may include travel bans, arms embargoes, export ban, etc.
Person	Natural and legal person
Sanctions Lists	Local Terrorist List and UN Consolidated List
STR/SAR	Suspicious Transaction Report / Suspicious Activity Report
Supervisory Authorities	Federal and local authorities which are entrusted by legislation to supervise FIs, DNFBPs, VASPs and non-profit organisations or the competent authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislation.
Supreme Council	Supreme Council for National Security
TFS	Targeted Financial Sanctions
UAE	United Arab Emirates
UN	United Nations
UN Consolidated List	United Nations Security Council Consolidated List pursuant to the relevant United Nations Security Council Resolutions.
UNSC	United Nations Security Council
UNSC Sanctions Committee	United Nations Security Council Sanction Committee that oversees the compliance of United Nations Security Council Resolutions. Please note that all current United Nations sanctions regimes have their own Sanctions Committee.
UNSCR	United Nations Security Council Resolution
VASPs	Virtual Assets Service Providers

Contents

Acronyms	1
Overview of Targeted Financial Sanctions	3
Section 1: Legal Framework	4
Section 2: What are TFS?	4
How long do these measures last?	5
Section 3: What is the Purpose of TFS?	5
Where to find the updated Sanctions Lists?	7
Who is the target of these measures?	7
What does 'funds or other assets' mean?	7
Section 4: Obligations on FIs, DNFBPs, and VASPs to Implement TFS	9
Step 1 – Subscribe	9
TFS Survey Feature	9
Step 2 – Screen	10
Step 3 – Apply Targeted Financial Sanctions	11
Step 4 – Report	12
Reporting TFS measures through GoAML	12
Reporting TFS by Email	15
Reporting STRs / SARs	16
Additional Obligations for FIs, DNFBPs, and VASPs	17
Section 5: Ownership, Control, and Acting on Behalf or at the Direction of	17
Majority Interest	17
Minority Interest	18
Control	19
Acting on Behalf or at the Direction of	20
Section 6: Enforcement of TFS	21
Consequences for FIs, DNFBPs, and VASPs	21
Exemption from Liability in Case of Good Faith TFS Implementation	22
Section 7: Requesting an Exemption or Permission to Access Frozen Funds or Other Assets	22
Frozen Funds or Other Assets due to the Local Terrorist List	22
Frozen Funds or Other Assets due to the UN Consolidated List	23
Section 8: Procedure to Cancel or Lift the Freezing Measures	26
Frozen Funds or Other Assets due to the Local Terrorist List	26
Frozen Funds or Other Assets due to the UN Consolidated List	27
Section 9: Requesting the Removal or De-listing of a Designation from the Local Terrorist List	28
Section 10: Requesting the Removal or De-listing of a Designation from the UN List	29
Contact us	29
Annex A: Frequency Asked Questions	30
Annex B: EO Notification / Alert System Subscription Guide	37
Document Version Update	41

Overview of Targeted Financial Sanctions

The United Nations Security Council (UNSC) is one of the six principal organs of the United Nations (UN) and has primary responsibility for the maintenance of international peace and security. It has 15 Members, and each member has one vote. Under the Charter of the United Nations, all Member States of the UN are obligated to comply with the Security Council decisions.

The UNSC holds the capacity to take action seeking to maintain or restore international peace and security under Article 41 of Chapter VII of the Charter of the United Nations by imposing sanctioning measures. These measures encompass a broad range of enforcement options that do not involve the authorisation of the use of armed force, including interruption of economic relations, international communications, and diplomatic relations.

The Security Council sanctions regimes focus mainly on supporting the settlement of political conflicts, nuclear non-proliferation, and counterterrorism. These regimes include measures ranging from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and restrictions on dealing with certain financial or commodity transactions.

In addition, the Financial Action Task Force (FATF), an inter-governmental body responsible for setting international standards on anti-money laundering (AML) and countering the financing of terrorism (CFT) and proliferation (CPF), under Recommendations 6 and 7 (R6/R7) of the FATF Standards, requires the implementation of targeted financial sanctions (TFS) to comply with the UN Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism, terrorism financing, and proliferation financing.

The United Arab Emirates (UAE), as a member of the United Nations, is committed to implementing UNSCRs, including those related to the UN's sanctions regimes. Consequently, through the Cabinet Decision No. 74 of 2020, the UAE is implementing relevant UNSCRs on the suppression and combating of terrorism, terrorist financing and countering the financing of proliferation of weapons of mass destruction, in particular relating to TFS. Persons should note that, in accordance with the laws of the UAE, the UAE Government also applies TFS by publishing a Local Terrorist List in accordance with UNSCR 1373 (2001).

The term TFS refers to asset freezing and other financial prohibitions, agreed upon by the UNSC, to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated individuals, entities, or groups.

This guidance is therefore focused on the procedures to implement local and UN sanctions by all Persons (natural and legal) in the UAE. Financial Institutions (FIs), Designated Non-Financial Businesses and Professions (DNFBPs), and Virtual Assets Service Providers (VASPs) are obliged, by UAE law, to apply policies, procedures and controls to implement TFS to those sanctioned and designated in the Local Terrorist List and UN Consolidated List (Sanctions Lists).

Section 1: Legal Framework

The following list comprises the relevant federal law and executive regulations issued so far for the purpose of implementing local and UN sanctions in the UAE.

Title	Articles/Text	Issued	Type
Federal Decree No. 26 of 2021 Amending Certain Provisions of Law No. 20 for 2018 on Anti-Money Laundering and Countering the Financing of Terrorism	16.1(e), 28	Issued: 2018 Amended: 2021	Federal Law
Cabinet Decision No. 10 of 2019 Concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations	7, 11, 12, 44.7, 60	2019	Executive Regulation
Cabinet Decision No. 74 of 2020 concerning the Local Terrorist List of terrorists and implementation of UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of mass destruction, and the relevant resolutions.	The whole text	2020	Executive Regulation

Section 2: What are TFS?

The term *targeted financial sanctions* includes both asset freezing without delay and prohibition from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

- **Asset freezing without delay:** Freezing is the prohibition to transfer, convert, dispose, or move any funds or other assets that are owned or controlled by designated individuals, entities, or groups in the Local Terrorist List or UN Consolidated List. It includes:
 - The freezing of funds and other financial assets and economic resources, and includes preventing their use, alteration, movement, transfer, or access.

- The freezing of economic resources also includes preventing their use to obtain funds or other assets or services in any way, including, but not limited to, by selling or mortgaging them.

Example:

- **FIIs:** a freezing measure can be suspending access to bank accounts or blocking transactions.
- **DNFBPs:** a freezing measure can be stopping the facilitation of or blocking the transfer of ownership of immovable or movable assets.
- **VASPs:** a freezing measure can be blocking services to trade and transfer virtual assets.

- **Prohibition from making funds or other assets or services available:** This means the prohibition to provide funds or other assets to or render financial or other services to, any designated individual, entity, or group.

Example:

- **FIIs:** offering banking or transactional services.
- **DNFBPs:** the provision of any services, such as legal services to transfer asset ownership, buying or selling real estate, selling jewellery, precious metals, natural resources, etc.
- **VASPs:** the provision of any services, including but not limited to trading and transferring virtual assets.

How long do these measures last?

Asset freezing and prohibition measures have **no time limit**: the funds or other assets should remain frozen, and the prohibition from making funds or other assets or services available remains until the individual, entity, or group is removed from the Local Terrorist List or the UN Consolidated List or until there is a freezing cancellation decision made by a competent authority or the UNSC.

Section 3: What is the Purpose of TFS?

The purpose of TFS is to deny certain individuals, entities, or groups the means to violate international peace and security, support terrorism or finance the proliferation of weapons of mass destruction. To achieve this, it seeks to ensure that no funds or other assets or services of any kind are made available to designated persons for so long as they remain subject to the targeted financial sanctions measures.

TFS are implemented in the UAE pursuant to UNSCRs in relation to:

- a) **Terrorism and terrorist financing:**

1. Islamic State in Iraq and the Levant (Da'esh), Al-Qaida, and associated individuals, groups, undertakings and entities.	UNSCR 1267 (1999) , 1989 (2011) and its successor resolutions
2. The Taliban, and associated individuals, groups, undertakings, and entities.	UNSCR 1988 (2011) and its successor resolutions
3. Any individual or entity included in the Local Terrorist List, pursuant to UNSCR 1373 (2001)	UNSCR 1373 (2001)

b) The proliferation of weapons of mass destruction (WMD):

1. Democratic People's Republic of Korea (DPRK): nuclear-related, other weapons of mass destruction-related and ballistic missile-related programmes.	UNSCR 1718 (2006) and its successor resolutions
2. Islamic Republic of Iran: nuclear programme	UNSCR 2231 (2015)

c) Other UN sanctions regimes with TFS:

1. Somalia	UNSCR 1844 (2008)
2. Iraq	UNSCR 1483 (2003)
3. Democratic Republic of Congo (DRC)	UNSCR 1596 (2005) & UNSCR 1807
4. Related to the involvement of terrorist bombing in Beirut (2005) plus restrictive measures in relation to UNSCR 1701 (2006) on Lebanon	UNSCR 1636 (2005) & UNSCR 1701 (2006)
5. Libya	UNSCR 1970 (2011)
6. Central African Republic (CAR)	UNSCR 2127 (2013)
7. South Sudan	UNSCR 2140 (2014)
8. Mali	UNSCR 2206 (2015)
9. Yemen	UNSCR 2374 (2017)

FIs, DNFBPs, and VASPs should note that TFS restrictions published in the Local Terrorist List and UN Consolidated List are subject to change. It is the obligation of all FIs, DNFBPs, and VASPs to ensure

relevant controls and procedures are in place to maintain relevant and up-to-date controls in order to effectively implement TFS restrictions.

Where to find the updated Sanctions Lists?

The information on designated individuals, entities, or groups in the Sanctions Lists is subject to change. The most recently updated information can be found in the following links:

- The UAE has a Local Terrorist List of all the sanctioned individuals, entities, or groups designated by the UAE Cabinet. The link to the Local Terrorist List can be found at the bottom of the Local Terrorist List webpage on the Executive Office's website: <https://www.uaieec.gov.ae/en-us/un-page#>
- The UNSC has a UN Consolidated List of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC. This link can be found on: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

Who is the target of these measures?

The freezing measures, including the prohibition of making funds or other assets or services available, apply to:

- a) Any individual, entity, or group designated in the Local Terrorist List issued by the Federal Cabinet or designated by the UNSC in the UN Consolidated List.
- b) Any entity, directly or indirectly owned or controlled by an individual, entity, or group designated under A.
- c) Any individual or entity acting on behalf of or at the direction of any individual, entity, or group designated under A & B.

In cases where an asset is owned or controlled in part or in full by a designated individual, entity, or group and such asset continues to produce benefit, for example in the form of dividends or interest, the relevant portion of such benefit is also subject to freezing measures.

What does 'funds or other assets' mean?

Funds or other assets: The term funds or other assets means any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.

Categories of funds: All types of funds or other assets are subject to freezing measures. The funds or other assets can be categorised into the following types:

1. Funds and Other Financial Assets

Funds and other financial assets subject to sanctions are, for example, the following:

- a. Cash, cheques, claims on money, drafts, money orders, bearer instruments, internet-based and other electronic or digital payment instruments, including virtual currencies.
- b. Deposits with FIs or other entities and balances on accounts, including but not limited to: (1) fixed or term deposit accounts, (2) balances on share trading accounts with banks, brokerage firms, or other investment trading accounts.
- c. Debts and debt obligations, including trade debts.
- d. Other accounts receivable, notes receivable, and other claims of money on others.
- e. Equity and other financial interest in a sole trader or partnership.
- f. Publicly and privately traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures, and derivatives contracts.
- g. Interest, dividends, or other income on or value accruing from or generated by assets.
- h. Credit, right of set-off, guarantees, performance bonds or other financial commitments.
- i. Letters of credit, bills of lading, bills of sale; notes receivable and other documents evidencing an interest in funds or financial resources and any other instruments of export-financing.
- j. Insurance and reinsurance.

2. Economic Resources

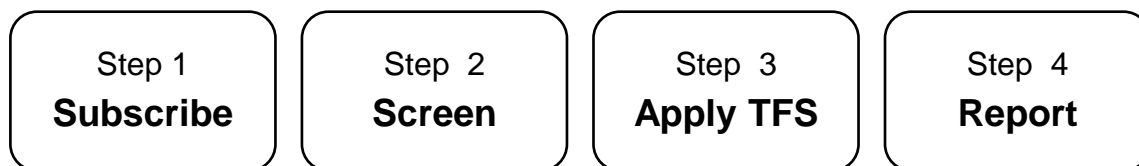
Economic resources subject to sanctions include assets of any kind, whether tangible or intangible, movable, or immovable, actual, or potential, which potentially may be used to obtain funds, goods, or services, such as:

- a. Land, buildings, or other real estate.
- b. Equipment, including computers, computer software, tools, and machinery.
- c. Office furniture, fittings and fixtures and other items of a fixed nature.
- d. Vessels, aircraft, and motor vehicles.
- e. Inventories of goods.
- f. Works of art, cultural property, precious stones, jewelry, or gold.
- g. Commodities, including oil, minerals, or timber.
- h. Arms and related material, including all items mentioned in the arms embargo, included but not limited to weapons and ammunition, military vehicles and equipment, paramilitary equipment, and spare parts for the aforementioned, and technical advice, assistance, or training related to military activities.
- i. Raw materials and components that can be used to manufacture improvised explosive devices or unconventional weapons, including but not limited to chemical components, detonating cord, or poisons.

- j. Patents, trademarks, copyrights, trade names, franchises, goodwill, and other forms of intellectual property; internet hosting or related services.
- k. Any other assets.

Section 4: Obligations on FIs, DNFBPs, and VASPs to Implement TFS

All FIs, DNFBPs, and VASPs must:



Step 1 – Subscribe

FIs, DNFBPs, and VASPs are required to subscribe to the Executive Office of the Committee for Goods & Material Subjected to Import and Export Control's (Executive Office or EO) Notification System on the Executive Office's website to receive automated email notifications on any updates to the Sanctions Lists: <https://www.uaieec.gov.ae/en-us/un-page>

This registration is aimed to help FIs, DNFBPs, and VASPs to receive updated and timely information about the designation and de-listing of individuals, entities, or groups in the Sanctions Lists.

For guidance on how to subscribe, refer to "Annex B: EO Notification System Subscription Guide".

TFS Survey Feature

The EO Notification System has been enhanced to include a TFS survey feature which provides a step-by-step guide for FIs, DNFBPs, and VASPs on their obligation to implement TFS as per Cabinet Decision No. 74 of 2020, including screening, freezing, and reporting. FIs, DNFBPs, and VASPs are encouraged to fill out the survey whenever a designation update is received.



Step 2 – Screen

FIs, DNFBPs, and VASPs must undertake regular and ongoing screening on the latest Local Terrorist List and UN Consolidated List. Screening must be undertaken in the following:

- Upon any updates to the Local Terrorist List or UN Consolidated List. In such cases, screening must be conducted immediately and without delay to ensure compliance with implementing freezing measures without delay (within 24 hours).
- Prior to onboarding new customers.
- Upon KYC reviews or changes to a customer's information.
- Before processing any transaction.

FIs, DNFBPs, and VASPs are also required to identify, assess, monitor, manage and mitigate terrorist and proliferation financing risks, particularly sanctions-related risks. The internal screening process must take into account such a risk assessment. Where there are higher risks, FIs, DNFBPs, and VASPs should take commensurate measures to manage and mitigate the risks, including applying enhanced screening measures. Correspondingly, where the risks are lower, they should ensure that the screening measures are commensurate with the lower level of risk. **FIs, DNFBPs, and VASPs must ensure full implementation of targeted financial sanctions in any risk scenario.**

The following databases must be included in the screening process:

- Existing customer databases. All systems containing customer data and transactions need to be mapped to the screening system to ensure full compliance.
- Potential customers before conducting any transactions or entering a business relationship with any Person.
- Names of parties to any transactions (e.g., buyer, seller, agent, freight forwarder, etc.)
- Ultimate beneficial owners, both natural and legal.
- Names of individuals, entities, or groups with direct or indirect relationships with them.
- Directors and/or agents acting on behalf of customers (including individuals with power of attorney).

Sanctions Lists contain a range of information to aid the identification of designated individuals, entities, or groups. The following are examples of the identifiers in the Sanctions Lists:

For natural person	For legal persons
<ul style="list-style-type: none"> • Name • Aliases • Date of birth • Nationality • ID or passport information • Last known address 	<ul style="list-style-type: none"> • Name(s) • Aliases • Address of registration • Address of branches • Other information
Potential match	<p>A potential match is when there is a partial match between identifiers in the Sanctions Lists with any information in your databases, and you are unable to conclude a false positive or a confirmed match.</p> <p>Example: Your customer's name and DOB match with the identifiers of a designated person in the Sanctions Lists, but the nationality is different and there is a slight difference in the name spelling.</p>

Confirmed match	A confirmed match is when an individual, entity, or group matches all of the key identifiers published on the Sanctions Lists.	Example: Your customer's name, nationality, and DOB fully match with the identifiers of a designated person in the Sanctions Lists, but the registered address is different.
False positive result	A false positive is a potential match to listed individuals, entities, or groups, either due to the common nature of the name or due to ambiguous identifying data, which on examination proves not to be a confirmed match.	Example: Your customer's name matches with a designated person who is 40 years old according to the DOB identifier in the Sanctions Lists, but your customer is a 16-year-old high school student.

Because many names are very common, you may find various potential matches. However, it does not necessarily mean that the individual, entity, or group you are dealing with is subject to TFS.

When identifying the potential match, by taking into consideration the knowledge you have of the customer, potential customer, beneficial owner, or transaction, through the customer due diligence and/or using reasonable information (e.g., open-source information, media articles, commercial databases, etc.), you must cross-check your customer's data with the identifiers published on the Sanctions Lists. If you are satisfied that the individual, entity, or group is not the designated individual, entity, or group, i.e. a '**False Positive Result**', then you do not need to implement any TFS measures. You may allow the transaction or business to continue its normal course, and you are required to maintain evidence of this process in your records.

If you are unable to internally verify whether the '**potential match**' is a false positive result or a confirmed match, then you must suspend any transaction and report the case to the Executive Office and the relevant Supervisory Authority and uphold the suspension measures until a response is received from the Executive Office on the status of the potential match (whether false positive or confirmed match). Reporting procedures on suspension measures due to potential matches are further explained in "Step 4 – Report".

If the individual, entity, or group matches all of the key identifiers published on the Sanctions Lists, then the result is considered a '**confirmed match**'. In case the confirmed match is an existing customer, you must freeze without delay, refrain from offering any funds or other assets or services and report the freezing measures to the Executive Office and the relevant Supervisory Authority within five business days from taking any freezing measure and/or attempted transactions. In case the confirmed match is a potential customer, you must reject the transaction immediately and report the case. Reporting procedures on freezing measures due to confirmed match are further explained in "Step 4 – Report".

Step 3 – Apply Targeted Financial Sanctions

The following are the TFS measures that must be implemented if a match with the Local Terrorist List or UN Consolidated List is identified.

- I. **Freeze all funds or other assets without delay:** freeze without delay (immediately or in any case within 24 hours) and without prior notice to the designated individual, entity, or group, all the funds or other assets:
 - a. Owned or controlled, wholly or jointly, directly, or indirectly, by an individual, entity, or group designated in the Local Terrorist List or the UN Consolidated List.

- b. Derived or generated from funds or other assets under item (a); or
- c. Any individual or entity acting on behalf of or at the direction of any designated individual, entity, or group.

The obligations to freeze without delay shall not prevent additions to frozen accounts of:

- interest, profits, or other earnings due on the account; or
- of payments due under contracts, agreements or obligations agreed upon prior to the date on which the account has become subject to freezing, provided such additions are immediately frozen.

- II. Prohibition of making funds or other assets or services available:** FIs, DNFBPs, and VASPs in the UAE are prohibited from providing funds or other assets to or rendering financial services or other services related to, whether in whole or in part, directly or indirectly, or for the benefit of any designated individual, entity, or group on the Local Terrorist List or on the UN Consolidated List.

Important: The obligation to implement targeted financial sanctions as per Cabinet Decision No. 74 of 2020 applies exclusively to individuals, entities, and groups designated on either the Local Terrorist List or UN Consolidated List. For designations on international sanctions lists (e.g. OFAC, UKHMT, EU, etc.), follow the instruction of your relevant Supervisory Authority on how to deal with matches to international sanctions lists.

Step 4 – Report

The mechanism to report any freezing or suspension measures taken upon identifying confirmed or potential matches is through the goAML platform. For non goAML users (Persons that do not fall under the definition of FIs, DNFBPs, or VASPs and are therefore not under an obligation to register on goAML), reporting should be made by sending an email to the Executive Office through iec@uaeiec.gov.ae.

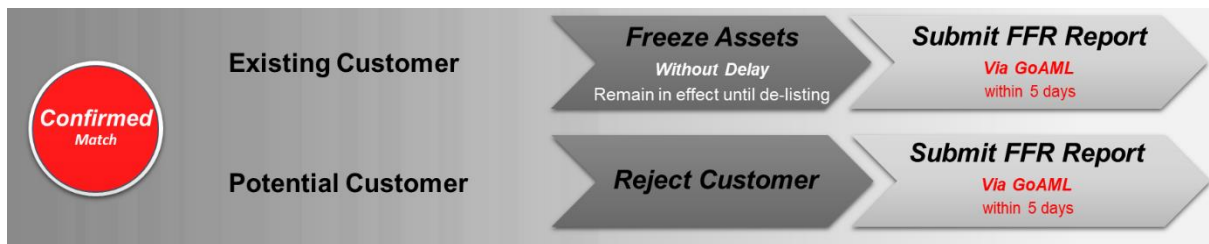
Reporting TFS measures through GoAML

The FIU, in collaboration with the Executive Office, has enhanced the goAML platform to allow FIs, DNFBPs, and VASPs to report freezing measures taken to implement TFS pursuant to Cabinet Decision No. 74 of 2020. The use of the goAML platform for TFS reporting purposes eases the burden of reporting on the FIs, DNFBPs, and VASPs since it utilizes a single platform for reporting, which many of the reporting entities are familiar with. The FIU has developed namely two additional reports: **Funds Freeze Report (FFR)** and **Partial Name Match Report (PNMR)**. Once the reporting entity raises the FFR or PNMR through goAML, the Executive Office and the relevant Supervisory Authority are notified at the same time.

Funds Freeze Report (FFR)

In case a confirmed match is identified, the reporting entity must freeze without delay (within 24hrs) all funds and other assets and submit a FRR through goAML within five business days of implementing the freezing measures, along with all the necessary information and documents regarding the confirmed match and the freezing measures taken. The following information is obligatory when submitting an FFR:

- **The full name of the 'confirmed match'.** Attach ID documents of the 'confirmed match', such as passport or other ID documents for individuals, and trade licenses and articles of association for entities.
- **Amount of funds or other assets frozen** (e.g., value of funds in bank accounts, value of transactions, value of securities, value of real estate, etc.). Attach proof documents such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc.



The examples below illustrate scenarios in which FIs, DNFBPs, and VASPs are required to submit FFRs and the type of information that should be included.

- **Financial Institutions**

Example 1: Bank

During the screening process, a bank identifies a full name match between a customer in its database (Person A) and a designated person on the Sanctions Lists. Person A's nationality and DOB also match with the designated person; however, the registered address is different. Person A has active current & savings accounts, a credit card, and a loan facility with the bank. In this case, Person A is considered to be a confirmed match. The bank must freeze without delay the current and savings accounts, credit card, and loan facility of Person A and submit a FFR in goAML. The FFR must include attachments that clarify:

- Amount of funds frozen in each account. Include supporting documents such as account statements.
- Amount of funds frozen in the credit card (e.g., limit on the credit card and the remaining balance). Include supporting documents such as credit card statements.
- Amount of funds frozen in the loan facility (e.g., total sum of the loan facility and the remaining balance).
- ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.

Example 2: Exchange House

An exchange house identifies a confirmed match (Person A) to the Sanctions Lists when screening its transactions database. Person A is attempting to make a transfer to a non-designated individual (Person B). The exchange house must freeze the transaction without delay and submit an FFR in goAML. The FFR must include attachments that clarify:

- The transaction amount frozen. Include supporting documents such as transaction receipt.
- ID documents of the confirmed match (Person A) and the recipient (Person B), such as ID card, travel documents, trade licenses, etc.

Example 3: Insurance

An insurance company identifies a confirmed match (Person A) when screening its customer database. Person A is the beneficiary of a life insurance policy. The insurance company must freeze the policy, including future premiums on receipt and any interest due to the account, and seek approval from the Executive Office – IEC before making any payments under the policy. The

insurance company must also submit an FFR in goAML with details of the insurance agreement (including policyholder, beneficiary, premiums, etc.)

Example 4: Brokerage

A brokerage company identifies a confirmed match (Person A) when screening its customer database. Person A owns a stock portfolio with the brokerage firm. Person A also receives dividends from the stocks owned. The brokerage company must freeze the stock portfolio without delay and submit an FFR in goAML. The FFR must include attachments that clarify:

- The quantity of the stocks frozen and their value. Include supporting documents such as portfolio summary.
- ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.

The brokerage company should credit any dividends due to Person A's account; however, the account must remain frozen, and the brokerage company must ensure that Person A is unable to sell his stocks or avail the dividends received.

• Designated Non-Financial Businesses & Professions

Example 1: Real Estate Brokers and Developers

A real estate broker identifies a confirmed match (Person A) when screening the parties to a property sale transaction. Person A is the prospective seller of the real estate. The real estate broker must block the transaction immediately, refrain from offering any services to Person A, and submit an FFR in goAML. The FFR must include attachments that clarify:

- The type, value, and location of the real estate being sold. Include supporting documents such as title deeds.
- ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.

Example 2: Dealer in Precious Metals & Stones (DPMS)

A DPMS identifies a confirmed match (Person A) when screening a prospective customer. Person A is attempting to sell high-value jewelry to the DPMS. The DPMS must immediately refrain from offering any services, including the sale or purchase of jewelry, to Person A and submit an FFR in goAML. The FFR must include attachments that clarify:

- Details of the attempted transaction, including the specifications and value of the jewelry attempted for sale.
- ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.

Example 3: Company Service Providers (CSPs)

A CSP identifies a confirmed match (Entity A) when screening its client database. Entity A is engaging the CSP for services to act as a formation agent. The CSP must immediately refrain from offering any services to Person A and submit an FFR in goAML. The FFR must include attachments that clarify:

- Details of the attempted transaction and formation agreement.
- ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.

• Virtual Asset Service Provider

Example 1: Cryptocurrency Exchange

A cryptocurrency exchange identifies a confirmed match (Person A) when screening its customer database. Person A owns multiple cryptocurrencies (Bitcoin, Ethereum, Ripple, etc.) in his exchange wallet. The cryptocurrency exchange must freeze the cryptocurrency assets in Person A's exchange wallet without delay and submit an FFR in goAML. The FFR must include attachments that clarify:

- The quantity of the cryptocurrency assets frozen and their value. Include supporting documents such as a portfolio summary.
- ID documents of the confirmed match, such as ID card, travel documents, trade licenses, etc.

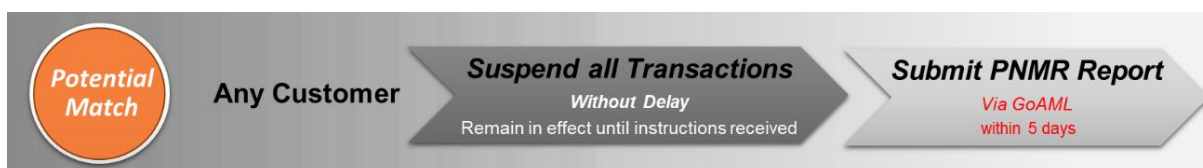
Funds Freeze Reports also cover previous transactions conducted by the confirmed match even if no current funds or other assets are held by the reporting entity. However, the reporting entity is required to clarify in the description of the FFR that no funds or other assets are currently being held by the reporting entity, and that the business relationship has ceased.

Partial Name Match Report (PNMR)

In case a potential match is identified, the reporting entity is required to suspend without delay any transaction, refrain from offering any funds, other assets or services, and submit a Partial Name Match Report (PNMR) through goAML, which will be received by the Executive Office and the relevant Supervisory Authority. The reporting entity must ensure all the necessary information and documents regarding the name match are submitted and maintain suspension measures related to the potential match until further instructions are received from Executive Office via goAML on whether to cancel the suspension ('false positive') or implement freezing measures ('confirmed match'). The following information is obligatory when submitting a PNMR:

- **The full name of the 'potential match'**. Attach ID documents of the 'potential match', such as passport or other ID documents for individuals, and trade licenses and articles of association for entities.
- **Amount of funds or other assets suspended** (e.g., value of funds in bank accounts, value of transactions, value of securities, value of real estate, etc.). Attach documentary proof such as bank statements, transaction receipts, securities portfolio summary, title deeds, etc.

Refer to the FAQ for the technical difference between freezing and suspending.



The examples provided for FFRs in the previous section, in terms of the suspension (freezing) measures and type of information required also apply when submitting PNMRs.

Reporting TFS by Email

For non goAML users (Persons that do not fall under the definition of FIs, DNFBPs, or VASPs and are therefore not under an obligation to register on goAML), the reporting of any freezing measures or attempted transaction by a designated individual, entity, or group must be communicated directly by email to the Executive Office through iec@uaeiec.gov.ae within five business days from implementing any freezing measures. The email must include information on the full name of the confirmed or potential match, and the value of funds or other assets frozen (attaching ID and documentary proof as listed above).

Reporting STRs / SARs

FIs, DNFBPs, and VASPs should be able to differentiate between cases that require submitting an FFR/PNMR, and between suspicious transactions and activities that require submitting an STR/SAR. Any suspicious transactions or activities that do not include confirmed or potential matches to the UAE Local Terrorist List or UN Consolidated List should be reported to the FIU by raising a STR/SAR through the goAML platform.

In the context of implementing TFS, reporting entities are advised to familiarize themselves with the TFS-related Reasons for Reporting (RFRs) in goAML. Below is a non-comprehensive list of TFS related RFRs when raising STRs/SARs:

- Customer is engaging in complex commercial deals and arrangements that seem to be aiming to hide the final destiny of the transaction/good or the beneficial owner, which could be a designated individual, entity, or group. (E.G: the use of a front company, middlemen, or intermediaries by the designated individual to circumvent the targeted financial sanctions).
- Customer is carrying out multiple ATM cash withdrawals in short succession across various locations in territories where sanctioned people have influence or around the border of sanctioned countries linked to terrorist financing.
- Customer is suspected to be working or acting on behalf of, or is controlled by, a sanctioned individual, entity, or group.
- Customer or transaction is suspected of being linked (directly or indirectly) to DPRK's nuclear-related, WMD-related, or ballistic missiles weapons program.
- Customer or transaction is suspected of being linked (directly or indirectly) to IRAN's nuclear weapons program.
- Customer or transaction is suspiciously involved in the supply, sale, delivery, export, or purchase of dual use, controlled, or military goods to countries of proliferation concerns or related to illegal armed groups.
- Transaction involves sale, shipment, or export of dual use goods incompatible with the technical level of the country to which it is being shipped.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- Inclusion of the individual/entity in the international sanctions list e.g. OFAC, UKHMT, EU, etc.

Example 1: UN Panel of Experts Report

After conducting screening, you have identified that a customer (Person A) is mentioned in a UN Panel of Experts Report. However, Person A is **not listed** in neither the UN Consolidated List nor the Local Terrorist List. In this case, you are not required to implement the TFS requirements since Person A is not listed locally or by the UNSC; however, the fact that Person A is mentioned in a UN Panel of Experts Report may be a cause for suspicion and you should consider raising an STR/SAR to the UAE FIU.

Example 2: International Sanctions

After conducting screening, you have identified that a customer (Person A) is subject to international sanctions. However, Person A is **not listed** in neither the UN Consolidated List nor the UAE Local Terrorist List. In this case, you are not required to implement the TFS requirements since Person A

is not listed locally or by the UNSC; however, the fact that Person A is subject to international sanctions may be a cause for suspicion and you should consider raising an STR/SAR to the UAE FIU.

Additional Obligations for FIs, DNFBPs, and VASPs

In addition to the above, FIs, DNFBPs, and VASPs must fulfill the following obligations:

1. **Cooperate** with the Executive Office and the relevant Supervisory Authority in verifying the accuracy of the submitted information.
2. **Implement the freezing, cancellation, or lifting decision**, when appropriate, without delay, pursuant to related UNSCRs or decisions of the Cabinet regarding issuance of the Local Terrorist List.
3. **Set and implement** policies, procedures, and internal controls to:
 - Ensure compliance with the obligations arising from Cabinet Decision No. 74 of 2020.
 - Identify the existing accounts, transactions, funds or other assets of designated individuals, entities, or groups.
 - Conduct ongoing TFS training and awareness sessions to relevant employees and senior management.
 - Adopt reasonable measures to consider beneficial owners, signatories, and powers of attorney with respect to accounts or transactions held by FIs, DNFBPs, or VASPs when searching for activities by designated individuals, entities, or groups.
 - Prohibit staff from, directly or indirectly, informing the customer or any third party that freezing action or any Other Measures are going to be implemented as per provisions of Cabinet Decision No. 74 of 2020.
 - Ensure having the appropriate resources to meet the obligations of implementing TFS.

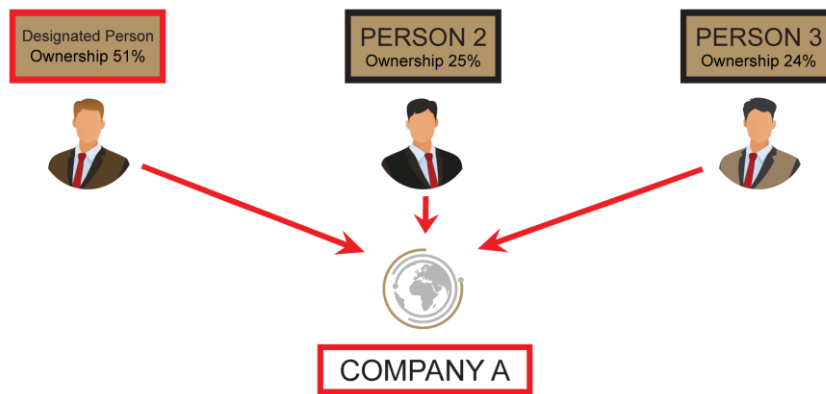
Section 5: Ownership, Control, and Acting on Behalf or at the Direction of

Majority Interest

FIs, DNFBPs, and VASPs are obligated to apply freezing measures on entities which are majority owned by designated individuals or entities.

In implementing TFS, the criterion to be taken into account when assessing whether a legal entity is majority **owned** by a designated individual or entity is the possession of more than 50% of the proprietary rights of the legal entity or having a controlling interest in it. If this criterion is satisfied, it is considered that the legal entity or arrangement is owned by another individual or entity and is subject to freezing measures.

Example: Person A is designated in the Sanctions Lists and owns 51% of non-designated Company A. Two other owners own 25% and 24% and are not designated. There is no legal evidence (e.g. power of attorney agreement) to suggest that the two other owners are acting on behalf of Person A. The funds or other assets of non-designated Company A must be frozen without delay since designated Person A owns more than 50% of non-designated Company A. However, the funds or other assets of the two non-designated owners must not be frozen since they are not designated and there is no legal evidence to suggest that they are acting on behalf of the designated Person A.

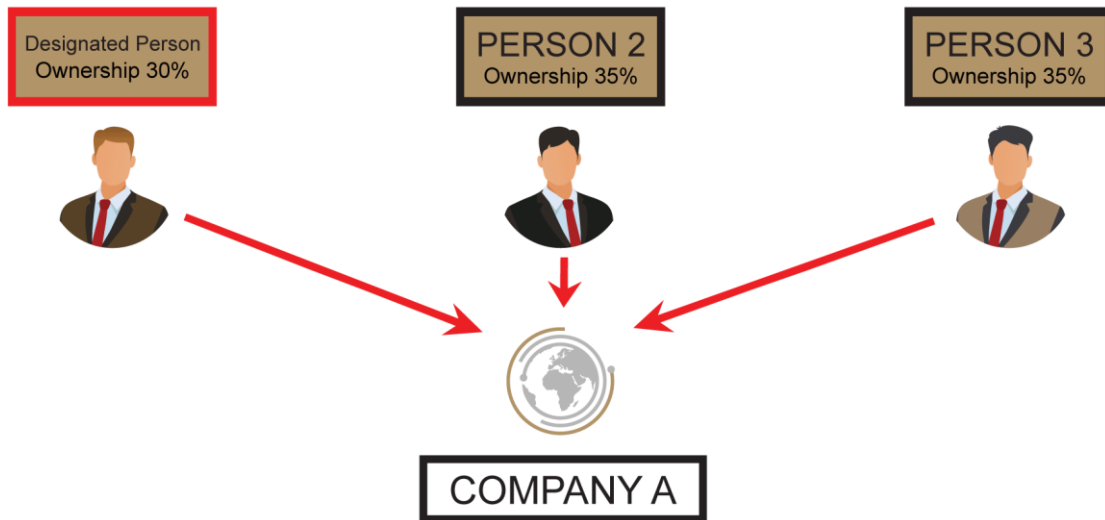


Minority Interest

A designated person holding 50% or less of the proprietary rights of a legal entity is considered to be holding a minority interest in the legal entity. In that case, the legal entity is not subject to freezing measures. However, FIs, DNFBPs, and VASPs must remain attentive to any changes in the ownership structure of the legal entity whereby the designated person's stake increases to greater than 50% or if they obtain a controlling interest. FIs, DNFBPs, and VASPs must also ensure that funds or other assets (e.g. profits, proceeds from sale of assets, etc.) due to the designated person are subject to freezing measures and are not made available under any circumstances.

Example: Person A is designated in the Sanctions Lists and owns 30% of non-designated Company A. Two other owners own the remaining 70% equally (35% each) and are not designated. There is no legal evidence (e.g. power of attorney agreement) to suggest that the two other owners are acting on behalf of Person A. The funds or other assets of non-designated Company A must not be frozen since designated Person A owns less than 50% of non-designated Company A and does not hold a majority interest. However, extreme vigilance is required to monitor any changes in the ownership structure in which Person A's stake in Company A increases to above 50% or if he obtains a majority interest. In addition, any funds or other assets due to Person A as a result of owning 30% of Company A must be subject to freezing measures. The funds or other assets of the two other owners must not

be frozen since they are not designated and there is no legal evidence to suggest that they are acting on behalf of the designated Person A.



Control

FIs, DNFBPs, and VASPs should apply freezing measures in cases in which a designated person holds a minority interest, if there is evidence that the designated person exerts control over the legal entity (despite owning a minority interest). The criteria to be taken into account when assessing whether a legal entity is mainly **controlled** by another person or entity, alone or pursuant to an agreement with another shareholder or other third party, could be any of the following:

- having the right to appoint or remove a majority of the members of the administrative or management body of such legal person, entity, group or arrangement;
- having appointed solely as a result of the exercise of one's voting rights a majority of the members of the administrative or management body of a legal person, entity, group or arrangement who have held office during the present and previous financial year;
- controlling alone, pursuant to an agreement with other shareholders in or members of a legal person, group or entity, a majority of shareholders' or members' voting rights in that legal person, entity, group or arrangement;
- having the right to exercise a dominant influence over a legal person, group or entity, pursuant to an agreement entered into with that legal person, entity, group or arrangement, or to a provision in its Memorandum or Articles of Association, where the law governing that legal person, entity, group or arrangement permits its being subject to such agreement or provision;
- having the power to exert the right to exercise a dominant influence referred to in point (d), without being the holder of that right;

- f. having the right to use all or part of the assets of that legal person, entity, group or arrangement;
- g. managing the business of that legal person, entity, group or arrangement on a unified basis, while publishing consolidated accounts;
- h. sharing jointly and severally the financial liabilities of legal person, entity, group, or arrangement, or guaranteeing them.
- i. Having a power of attorney or authorized signatory arrangement over a legal person, entity, or group.

Example 1: Person A is designated in the Sanctions Lists and owns 30% of non-designated Company A. Two other owners own the remaining 70% equally (35% each) and are not designated. Person A has a signed agreement with the two other owners that gives Person A majority voting rights in Company A. Despite Person A holding a minority interest, the funds or other assets of Company A must be frozen without delay since the signed agreement between Person A and the other owners proves that Person A exerts control over Company A by holding majority of the voting rights.

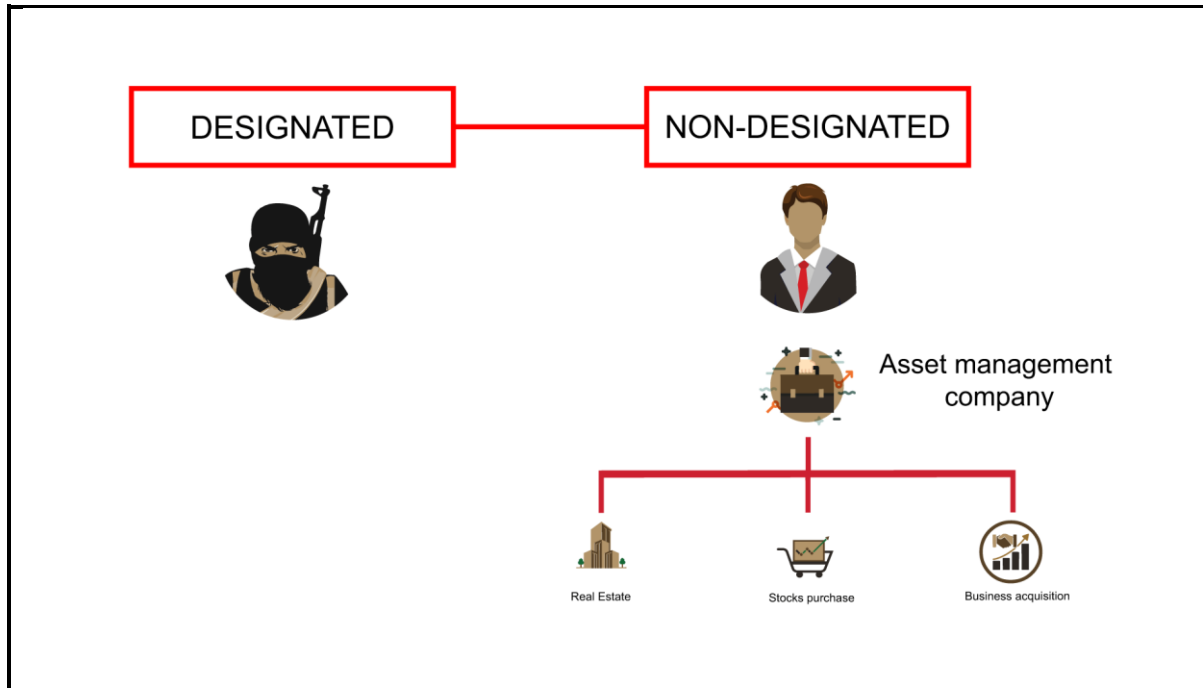
Example 2: Person A is designated in the Sanctions Lists and has a power of attorney to act on behalf of Person B and is also the authorized signatory. The funds and other assets of Person B must be frozen without delay since the power of attorney and authorized signatory arrangement is evidence that Person A possesses control over the funds or other assets of Person B.

Important: If an FI, DNFBP, or VASP implements freezing measures based on the 'control' criteria, it must rely on evidence-based documentation (e.g. legal agreements, guarantor agreement, provision in the Articles of Association, power of attorney or authorized signatory, etc.) that proves that the designated person exerts control over the legal entity. Freezing measures must not be applied relying on suspicion only.

Acting on Behalf or at the Direction of

FIs, DNFBPs, and VASPs are required to implement targeted financial sanctions on individuals or entities acting on behalf or at the direction of designated persons. The relationship to act on behalf or at the direction of designated persons must be evidenced by legal documentation, such as a power of attorney or authorized signatory.

Example: Person A is designated in the Sanctions Lists. Person B has a power of attorney to act on behalf of Person A and runs an asset management company where Person A is the beneficial owner. The funds and other assets of Person B must be frozen without delay since the power of attorney is evidence that Person B is acting on behalf or at the direction of designated Person A.



Important: If an FI, DNFBP, or VASP implements freezing measures based on the ‘acting on behalf or at the direction of’ criteria, it must rely on evidence-based documentation (e.g. power of attorney, authorized signatory, etc.) that proves that the individual or entity is acting on behalf or at the direction of the designated person. Freezing measures must not be applied relying on suspicion only.

Section 6: Enforcement of TFS

Consequences for FIs, DNFBPs, and VASPs

Any Person, found to violate and/or be in non-compliance with the obligation in the Cabinet Decision No. 74 of 2020 or failing to implement procedures to ensure compliance may face imprisonment of no less than one year and no more than seven years and/or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham).

In addition, FIs, DNFBPs, and VASPs are subject to supervision, and in the case of identified non-compliance, Supervisory Authorities can apply the enforcement actions set out under Article (14) of Federal Decree No. 26 of 2021 Amending Certain Provisions of Law No. 20 for 2018 on Anti-Money Laundering and Countering the Financing of Terrorism. The Supervisory Authorities of the FIs, DNFBPs, and VASPs have the legal capacity to supervise the implementation of TFS. The Supervisory Authorities may also issue the following administrative sanctions:

- a. Letter of warning.
- b. Administrative penalties of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) for each violation.
- c. Banning the violator from working in the sector related to the violation for the period determined by the Supervisory Authority.

- d. Constraining the powers of the board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of a temporary inspector.
- e. Suspend managers, board members and supervisory and executive management members who are proven to be responsible for the violation for a period to be determined by the Supervisory Authority or request their removal.
- f. Suspend or restrict the activity or the profession for a period to be determined by the Supervisory Authority.
- g. Cancel the License.

Exemption from Liability in Case of Good Faith TFS Implementation

An FI, DNFBP, or VASP who, in good faith, freezes funds or other assets, denies disposal thereof, or refuses to provide financial services relating to designated individuals, entities, or groups, or declined to perform any other obligation (including reporting obligations) in compliance with the provisions of Cabinet Decision No. 74 of 2020 shall be exempt from any damages or claims, resulting from such actions, including penal, civil, and/or administrative liability.

Section 7: Requesting an Exemption or Permission to Access Frozen Funds or Other Assets

Frozen Funds or Other Assets due to the Local Terrorist List

An individual, entity, or group designated in the Local Terrorist List, or his/her legal representative, and any stakeholder may request access to all or part of the frozen funds or other assets for any of the following purposes:

- a. To cover **necessary** or **basic** expenses (including for humanitarian needs), such as the amounts payable for foodstuffs, rent, mortgage, medicine, medical treatment, insurance premiums, educational and judicial fees, and public utility fees.
- b. To pay **professional fees** and costs relating to rendered legal services and other **extraordinary expenses** within reasonable limits, or services relating to safekeeping or management of frozen funds or other assets.

The procedure to request permission to use the frozen funds or other assets is the following:

1. Send a written request to access all or part of the frozen funds or other assets accompanied with all supporting documents to the Executive Office by email to iec@uaeiec.gov.ae.
 - Follow the procedures and attach all supporting documents to substantiate your claim, as stated at <https://www.uaeiec.gov.ae/en-us/un-page>
2. The Executive Office will send the request to the Ministry of Justice for its consideration in coordination with the Supreme Council.

3. The Ministry of Justice may approve or reject the use of the frozen funds or other assets, in part or in whole.
4. The Executive Office will notify the applicant, in writing, of the approval or rejection of the request.

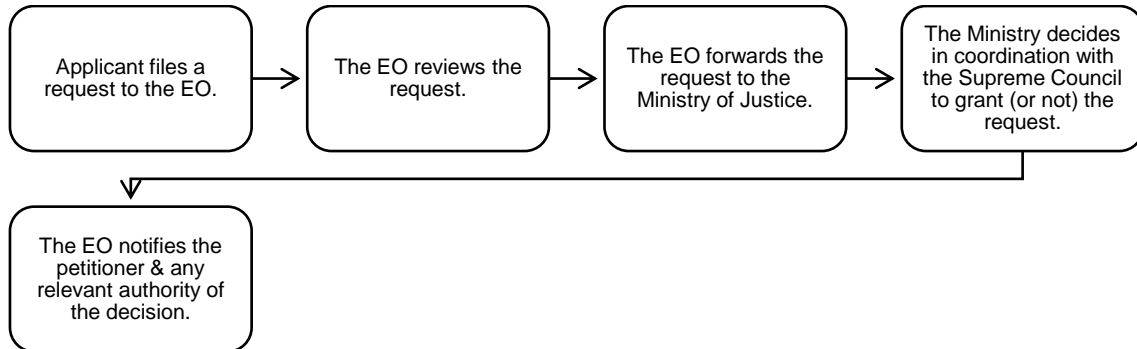


Exhibit 1: Procedure to request permission to use funds or other assets subject to Local Terrorist List

Grievances to the court

In case the application is rejected, or if no response to it is received after 30 days from the date of its submission, the applicant may file a grievance before the Competent Court within 30 days from the date when he/she was notified of the rejection, or after the response period of 30 days has elapsed.

The applicant may not appeal against the rejection of the request until a grievance against it is duly filed and rejected, or the period for responding to it has elapsed, and the applicant has notified the Executive Office and Competent Court of its intention to appeal the ruling.

Frozen Funds or Other Assets due to the UN Consolidated List

Any individual, entity, or group affected by a freezing measure may submit a written request to unfreeze all or part of the funds or other assets to the Executive Office. This request must be submitted by the affected person or his/her legal representative, accompanied by all supporting documents.

1. To cover basic expenses:

The Executive Office may consider a request for access to funds or other assets frozen as per the UN Consolidated List, in the following cases:

- a. To cover **necessary** or **basic** expenses (including for humanitarian needs), such as the amounts payable for foodstuffs, rent, mortgage, medicine, medical treatment, taxes, insurance premiums, educational and judicial fees, and public utilities fees.
- b. To pay **professional fees** and costs relating to rendered legal services within reasonable limits or services relating to safekeeping or management of frozen funds.

The procedure to request permission to access the frozen funds or other assets is the following:

1. Submit a written request to the Executive Office by email iec@uaeiec.gov.ae accompanied with all supporting documents.
 - Follow the procedures and attach all supporting documents to substantiate your claim stated in <https://www.uaeiec.gov.ae/en-us/un-page>
2. The Executive Office reviews the request.
3. The Executive Office notifies the relevant UNSC Sanctions Committee of its intention to approve the request.
4. The Executive Office may decide to grant the request upon no objection or other notification from the UNSC or relevant UNSC Sanctions Committee.
5. The Executive Office notifies the applicant and the relevant Supervisory Authority.

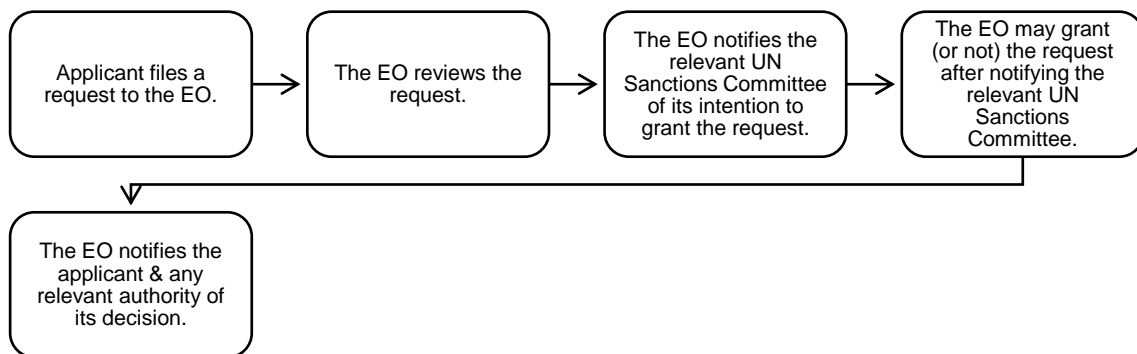


Exhibit 2: Procedure to request permission to use funds subject to the UN Consolidated List for the purposes of basic expenses

The Executive Office may revoke the decision to use funds or other assets frozen at any time and when having reasonable grounds for a suspicion that the funds are used for any purpose other than permitted, in writing, in the approved application request.

2. To cover extraordinary expenses

The Executive Office may forward the request to the relevant UNSC Sanctions Committee to access funds frozen as per the UN Consolidated List, in the following cases:

- To cover **extraordinary** expenses, other than those mentioned under the basic expenses section above.

The Executive Office will notify the relevant UNSC Sanctions Committee of the request to approve the submitted application and may only approve such request upon obtaining a written approval from the UNSC Sanctions Committee. In the absence of a written approval, the Executive Office will not grant the request.

The Executive Office will notify in writing the applicant or his/her legal representative of the decision to enable use of the frozen funds.

The procedure to request permission to access the frozen funds is the following:

1. Submit a written request to the Executive Office through email to iec@uaeiec.gov.ae accompanied with all supporting documents.
 - Follow the procedures and attach all supporting documents to substantiate your claim stated in <https://www.uaieic.gov.ae/en-us/un-page#>
2. The Executive Office reviews the request.
3. The Executive Office forwards the request to the relevant UNSC Sanctions Committee.
4. The UNSC Sanctions Committee decides on the requests and notifies the Executive Office.
5. The Executive Office notifies the applicant and the relevant Supervisory Authority.

The Executive Office may revoke the decision to use funds frozen under the Sanctions Lists at any time and when having reasonable grounds for a suspicion that the funds are used for financing terrorism or financing proliferation of weapons of mass destruction.

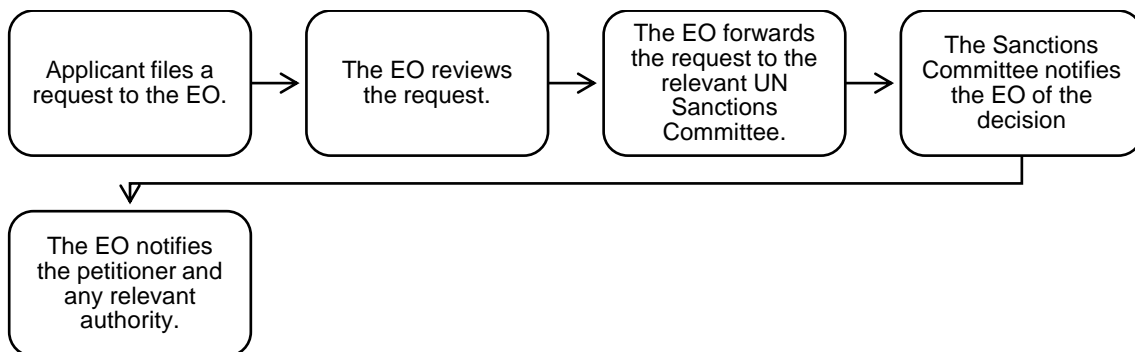


Exhibit 3: Procedure to request permission to use funds or other assets subject to the UN Consolidated List for the purposes of extraordinary expenses

Grievances to the court

If the application for use of funds frozen under the Sanctions Lists is rejected or remains without response for thirty (30) days from date of its submission, the applicant may file a grievance before the Competent Court within sixty (60) days from the date on which he/she was notified of the rejection of the application, or after the response period elapses.

The Court's decision on the grievance may not be appealed, and if the court rules to reject the grievance, a new grievance may only be filed after six (6) months from the date of rejection of the grievance, unless a serious reason that is accepted by the President of the Court arises before the expiry of such period.

An appeal against a decision to refuse the use of frozen funds shall not be accepted before a grievance against it is filed and rejected, or before the period given to respond expires.

Section 8: Procedure to Cancel or Lift the Freezing Measures

Freezing procedures and Other Measures may be lifted when taken against an individual, entity, or group who was adversely affected under the following situations:

- An individual, entity, or group that has a name identical or similar to a designated individual, entity, or group;
- The designated individual, entity, or group has been removed from the list by the relevant authorities; or
- The individual, entity, or group is a third party acting in good faith who has been adversely or wrongly affected by the freezing measures.

Frozen Funds or Other Assets due to the Local Terrorist List

The procedure for cancellation of freezing and any Other Measures taken against an individual, entity, or group with a name identical or similar to an individual, entity, or group designated, or the person who has been adversely affected by the freezing or any of the Other Measures due to being designated in the Local Terrorist List, is the following:

1. Submit a written application to the Executive Office accompanied with all supporting documents to the email: iec@uaeiec.gov.ae.
 - Follow the procedures and attach all supporting documents to substantiate your claim stated online at <https://www.uaeiec.gov.ae/en-us/un-page>
2. The Executive Office reviews the request and forwards it to the Supreme Council for its decision.
3. The Executive Office notifies the applicant and the relevant Supervisory Authority.

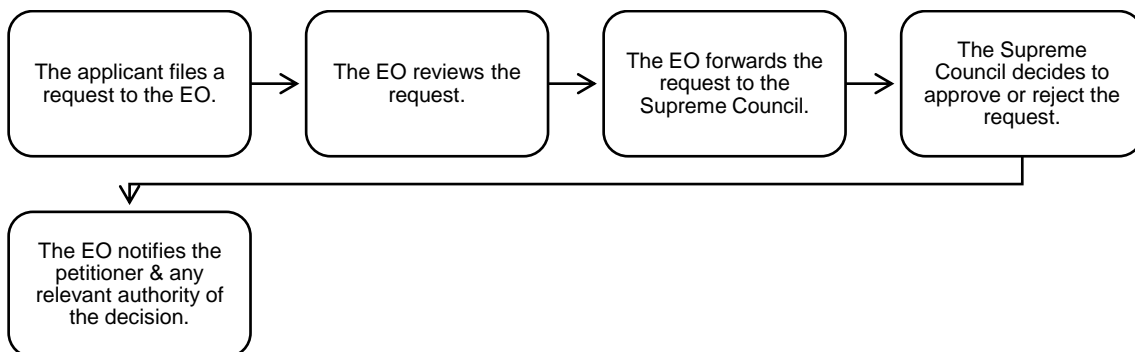


Exhibit 4: Procedure to request the cancellation of freezing and/or other TFS measures as designated by the Local Terrorist List

Grievances to the court

If the application is rejected by the Supreme Council, or if no response to the application is received within thirty (30) days from date of its submission, the applicant may file a grievance before the Competent Court within sixty (60) days from the date of notification of the rejection, or after the response period has elapsed.

The court's decision on the grievance may not be appealed, and if the court rules to reject the grievance, a new grievance may only be filed after six (6) months from the date of rejection of the grievance, unless a serious reason that is accepted by the President of the Court arises before the expiry of such period.

Frozen Funds or Other Assets due to the UN Consolidated List

The procedure for cancellation of freezing and any Other Measures taken against an individual, entity, or group with a name identical or similar to an individual, entity, or group designated, or the person who has been adversely affected by the freezing or any of the Other Measures due to being designated in the UN Consolidated List, is the following:

1. Submit a written application to the Executive Office accompanied with all supporting documents.
 - Follow the procedures and attach all supporting documents to substantiate your claim stated in <https://www.uaieic.gov.ae/en-us/un-page>
2. The Executive Office reviews the request and decides whether to grant the request.
3. The Executive Office notifies the applicant and the relevant Supervisory Authority.

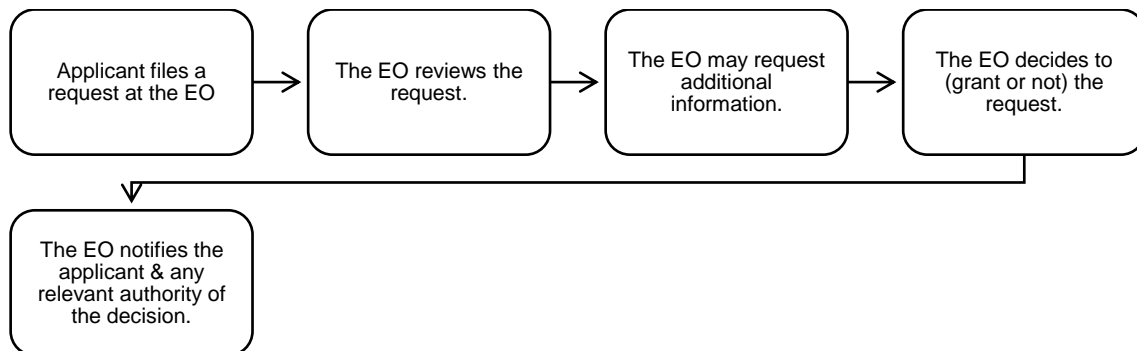


Exhibit 5: Procedure to request the cancellation of freezing and/or other TFS measures subject to the UN Consolidated List

Grievances to the court

If the request to lift freezing and Other Measures is rejected or remains without a response for thirty (30) days from the date of its submission, the applicant may file a grievance before the Competent Court within sixty (60) days from the date on which he/she was notified of the rejection of the request, or after the response period elapses.

The court's decision regarding the grievance shall not be subject to appeal. If a grievance is rejected, a new grievance may only be submitted after six (6) months from the date of rejection of the previous grievance, unless a serious reason that is accepted by the President of the Court arises before the expiry of such period.

Section 9: Requesting the Removal or De-listing of a Designation from the Local Terrorist List

Any individual, entity, or group designated in the Local Terrorist List can submit a grievance against the designation decision. The request for removal can also apply for:

- A deceased individual; or
 - An entity that no longer exists.
1. Submit an application to the Executive Office, attaching thereto all documents supporting the grievance.
 - Attach all supporting documents to substantiate your claim by email to iec@uaeiec.gov.ae
 2. The Executive Office shall refer the request to the Supreme Council.
 3. The Supreme Council communicates the request to the Cabinet for its decision.
 4. The Executive Office notifies the applicant and relevant authorities.

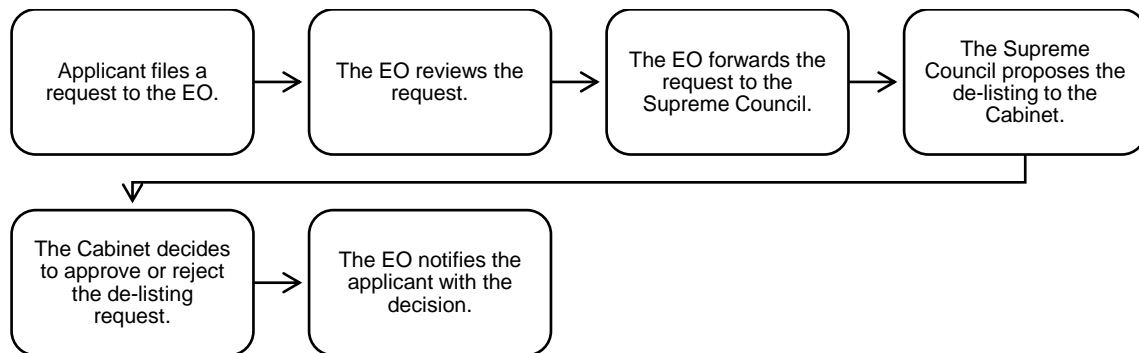


Exhibit 6: Procedure to request the removal or de-listing from the Local Terrorist List

Grievances to the court

In case the grievance was rejected or remains without a response for sixty (60) days from date of its submission, the grievant may challenge the Cabinet's designation decision before the Competent Court within sixty (60) days from the date he was notified of the rejection or lapse of the response period.

The court's decision regarding the grievance shall be incontestable. If a grievance was rejected, a new grievance may only be submitted after the lapse of six (6) months from date of rejection of the previous grievance, unless a serious reason acceptable to the President of the Court arises before expiry of such period.

Section 10: Requesting the Removal or De-listing of a Designation from the UN List

Any individual, entity, or group designated by the UNSC can submit a request for removal from the UN Consolidated List to the applicable UNSC Sanctions Committee, following the procedures for submitting de-listing requests pursuant to each UNSC Sanctions Committee.

Individuals, entities, or groups designated in UNSC Sanctions Lists can submit de-listing requests directly to the **Focal Point for De-listing** (except for designated individuals, entities, or groups inscribed on the list of the 1267/1989/2253 Committee ("the ISIL (Da'esh) and Al-Qaida Sanctions List"). Designated individuals or entities seeking to de-list from the Security Council's ISIL (Da'esh) and Al-Qaida Sanctions List must submit their petition to **The Office of the Ombudsperson**.

De-listing procedures include, for example:

- ❖ [1718 Sanctions Committee - Democratic People's Republic of Korea](#)
- ❖ [1988 Sanctions Committee - The Taliban, and associates](#)
- ❖ [For other UN Sanctions Committees](#)
- ❖ [Focal Point for De-listing](#)

De-listing procedures related to ISIL (Da'esh) and Al-Qaida Sanctions include, for example:

- ❖ [UNSCR 1267 \(1999\), 1989 \(2011\) de-listing procedure](#)
- ❖ [Ombudsperson to the ISIL \(Da'esh\) and Al-Qaida Sanctions Committee](#)

The request for removal can also apply for:

- A deceased individual; or
- An entity that no longer exists.

For detailed procedures on Focal Point De-listing, please visit the UN's webpage on [Procedures of the Focal Point for De-listing](#) and refer to the informal and unofficial [flowchart](#) that aims to provide a visual guide to the focal point process.

For detailed procedures on de-listing from "the ISIL (Da'esh) and Al-Qaida Sanctions List", please visit the UN's webpage on [Procedure for requests for delisting submitted to the Office of the Ombudsperson](#) and refer to the [flowchart](#) for an overview of the procedure.

Contact us

Send an email to contact the Executive Office of the Committee for Goods and Materials Subject to Import and Export Control to iec@uaeiec.gov.ae.

Annex A: Frequency Asked Questions

1. What does 'targeted financial sanctions' ("TFS") mean?

The term targeted sanctions means that such sanctions are imposed against specific individuals, entities, or groups. The term TFS includes both asset freezing without delay and prohibition from making funds or other assets or services, directly or indirectly, available for the benefit of sanctioned individuals, entities, or groups.

2. Why are individuals, entities, or groups designated in the Sanction Lists?

The Sanction Lists include names of individuals, entities, or groups that the UAE or the UN believe are detrimental to national and/or global peace and security. These individuals, entities, or groups are mostly involved in acts of terrorism, terrorism financing, proliferation financing, and violation of international law.

3. What does 'freezing' mean?

Freezing means to prohibit the transfer, conversion, or movement of any funds or other assets that are owned or controlled by a designated individual, entity, or group in the Sanctions Lists.

4. What is the difference between 'freezing' and 'suspending'?

Freezing and suspension measures follow the same procedures operationally (both are preventive measures that aim to stop the designated individual, entity, or group from gaining access to funds or other assets).

Suspending indicates that the reporting entity has come across a 'potential match' and is not sure whether the individual, entity, or group is certainly designated. The suspension measures should remain in place until further instructions are received from the Executive Office.

Freezing indicates that the reporting entity has come across a 'confirmed match' and the freeze measures must remain in place until the designated individual, entity, or group is de-listed from Sanctions Lists or upon further instructions received from the Executive Office.

5. What does 'without delay' mean?

'Without delay' means applying freezing measures immediately upon identifying a match to the Sanctions Lists or in any case within 24 hours upon designation of an individual, entity, or group on the Sanctions Lists.

6. What does 'funds or other assets' mean?

Any assets, including, but not limited to, financial assets, economic resources (including oil and other natural resources), property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit,

and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services.

7. What is the legal framework for the implementation of TFS in the UAE?

Article 16(e) of Federal Law No. 20 of 2018 (amended by Federal Decree No. 26 of 2021) requires the prompt application of the directives when issued by the competent authorities in the state for implementing the decisions issued by the UN Security Council under Chapter (7) of UN Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction, and other related directives.

In addition, the UAE issued the Cabinet Decision No. 74 of 2020, establishing the framework regarding TFS, including the Local Terrorist List and the UN Consolidated List and the procedures to implement TFS.

8. Who must comply with TFS?

Sanctions restrictions, including TFS measures, must be implemented by any Person (both natural and legal entities), including government authorities and FIs, DNFBPs, and VASPs located in the UAE and operating within the UAE's jurisdiction.

9. Cabinet Decision No. 74 of 2020 requires implementing TFS on which sanctions lists?

The scope of Cabinet Decision No. 74 of 2020 in implementing TFS covers the UAE Local Terrorist List and UN Consolidated List **only**. International sanctions lists are out of the scope of the Cabinet Decision.

10. How can I find out who is a designated individual, entity, or group?

You can find out who are the designated individuals, entities, or groups by checking the updated Sanctions Lists in the links below:

- The link to the UN Consolidated List: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>
- The link to the Local Terrorist List can be found at the bottom of the Local Terrorist List webpage on the Executive Office's website: <https://www.uaieec.gov.ae/en-us/un-page#>

11. Is there an excel format of the UAE Local Terrorist List?

Yes. The excel format of the UAE Local Terrorist List can be found under the 'Sanctions Implementation' section of the Executive Office's website <https://www.uaieec.gov.ae/en-us/un-page#>

12. What actions must FIs, DNFBPs, or VASPs take if funds or other assets of designated individuals, entities, or groups are detected?

In case an FI, DNFBP, or VASP determines that any of the funds or other assets it holds or administers belong to designated individuals, entities, or groups, it shall take the following steps to implement TFS:

- a) Freeze all funds or other assets without delay, and any funds or other assets derived or generated from such funds or other assets, without providing any notice to the customer or potential customer prior to taking the freezing measures.
- b) Refrain from providing any financial or other services or from providing funds or other assets to or for the benefit of a designated individual, entity, or group.
- c) Report to the Executive Office and the relevant Supervisory Authority within five days of the freezing measures taken through goAML, including information on the status of and any action taken with respect to assets, the nature of assets and amount of assets frozen, and any other information that is relevant to or would facilitate compliance with Cabinet Decision No. 74 of 2020.
- d) Fully cooperate with the Executive Office and the relevant Supervisory Authority in verifying the accuracy of the information provided.

13. What if my customer's name does not match the name of the designated individual or entity?

In case of a 'potential match' with a designated individual or legal entity, an FI, DNFBP, or VASP must first conduct an internal check on whether the potential match is a designated person. If the FI, DNFBP, or VASP is satisfied that the 'potential match' is not an individual or entity subject to TFS ('false positive result') after conducting the internal check, then it can allow for the business relationship to proceed while keeping an internal record of the case.

If the FI, DNFBP, or VASP is unable to verify whether the 'potential match' is a confirmed match or a false positive, then it must suspend any transaction and report it to the Executive Office by submitting a PNMR through goAML. The suspension measures must remain in place until further instructions are received from the Executive Office.

14. If I identify a confirmed or potential match, how should I report it?

If you identify a confirmed match, you must freeze without delay and report by submitting a **Funds Freeze Report (FFR)** through goAML. The FFR must include details on the type and amounts of funds or other assets frozen, ID documents of the confirmed match, and any other supporting documents.

If you identify a potential match, you must suspend without delay and report by submitting a **Partial Name Match Report (PNMR)** through goAML. The PNMR must include details on the type and amounts of funds or other assets suspended, ID documents of the potential match, and any other supporting documents.

15. Do I need to report confirmed or potential matches separately to my Supervisory Authority?

No. FFRs and PNMRs submitted through goAML are received simultaneously by the Executive Office and your relevant Supervisory Authority.

16. Should I report previous transactions or business dealings with confirmed or potential matches?

Yes. You must report any previous transactions of designated persons, even if you do not currently hold any funds or other assets or provide any services to the designated person.

The FFR or PNMR must clearly state that no funds or other assets are currently held, and no services are currently being provided to the designated person.

If the designated person has never conducted a transaction with or through you, or you have never held any funds or other assets of the designated person, or you have never provided any products or services assets to the designated person during the life of the business relationship, this should be made clear.

17. Am I under an obligation to register in goAML?

Any Person (natural or legal) that performs activities which fall under the definition of FIs, DNFBPs, or VASPs as per UAE legislation **has an obligation to register on goAML** to be able to submit suspicious transactions/activity reports (STRs/SARs) to the UAE FIU, as well as to submit TFS reports (FFRs/PNMRs) to the Executive Office and the relevant Supervisory Authority.

FIs and DNFBPs that are not registered on goAML face the risk of being subject to administrative and/or financial sanctions by the relevant Supervisory Authority for failure to register on goAML.

Please contact your relevant Supervisory Authority and the UAE FIU for instructions on how to register.

18. How should I report a confirmed or potential match if I am not a goAML user?

If you identify a confirmed or potential match, and you are not a goAML user (Persons that do not fall under the definition of FIs, DNFBPs, or VASPs and are therefore not under an obligation to register on goAML), then you must report it by sending an email to the Executive Office on iec@uaeiec.gov.ae with details of the case and attaching all supporting documentation.

Registered goAML users must always report a confirmed or potential match using goAML.

19. If I identify that a customer is subject to international sanctions, however, the customer is not listed on the UAE Local Terrorist List nor the UN Consolidated List. Should I report it by raising an FFR or PNMR?

No. FFRs and PNMRs are used only to report confirmed or potential matches to the UAE Local Terrorist List or the UN Consolidated List.

For designations on international sanctions lists (e.g., OFAC, UKHMT, EU, etc.), follow the instruction of your relevant Supervisory Authority on how to deal with matches to international sanctions lists.

20. What are the consequences in case of a failure to comply with the obligations set out in Cabinet Decision No. 74 of 2020, other applicable legislation and this guidance note?

Any Person, found to violate and/or be in non-compliance with the obligation in the Cabinet Decision No. 74 of 2020 or failing to implement procedures to ensure compliance may face imprisonment of no less than one year and no more than seven years and/or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham).

In addition, Supervisory Authorities can impose appropriate administrative sanctions (e.g., ranging from warning letter to license cancellation) when there is a violation or shortcoming in implementing TFS obligations.

21. Can I be held liable for freezing funds of a designated individual or entity based on the Cabinet Decision?

The Cabinet Decision clearly states that any individual or entity is exempted from criminal, administrative, or civil liability if a freezing measure is carried out in good faith and for the purpose of complying with the provisions of the Cabinet Decision. Thus, as long as the freezing measures were taken based on the belief that the relevant funds are targeted funds, the individual or entity, FI, DNFBP, or VASP is exempted from any liability resulting from such freezing measure even if it later turns out that the frozen funds are in fact not targeted by the Cabinet Decision.

At the same time, FIs, DNFBPs, and VASPs shall note that the criminal sanctions may apply to any Person who violates or fails to comply with the freezing obligation. Accordingly, both intentional and gravely negligent conduct resulting in the lack of application of a freezing measure may trigger administrative sanctions and/or criminal liability.

22. Can permission be obtained to access frozen assets by the designated individual or entity?

For the UN Consolidated List, the Executive Office, in limited circumstances, may permit access to frozen funds based on a request by the designated individual or entity. The applicant will, in such case, receive a written statement from the Executive Office stating the amount and conditions of access to the assets.

For the Local Terrorist List, the Ministry of Justice may permit access to frozen funds in some limited circumstances based on a request by the designated individual or entity or any affected third party. The applicant will, in such case, receive a written statement from the Ministry of Justice stating the amount and conditions of access to the assets.

23. May I permit transfers to be made into frozen accounts, and if so, which ones are subject to what conditions?

The Cabinet Decision provides that FIs, DNFBPs, or VASPs may credit frozen accounts with interest or other earnings on those accounts; or with payments due under contracts, agreements, or obligations that were concluded or arose before the date on which the individual or entity was designated, provided that any additions to such accounts shall also be frozen.

The Executive Office and the relevant Supervisory Authority must be notified about such transactions by submitting an FFR through goAML with information and supporting documentation on the additional amounts added to the account.

24. How can I determine whether I am in possession of targeted funds?

FIs, DNFBPs, and VASPs are responsible for having in place effective processes, policies and procedures to implement the provisions of the Cabinet Decision No. 74 of 2020. This involves frequently checking customer databases and any information obtained on potential or existing customers against Sanctions Lists to determine whether an FI, DNFBP, or VASP possesses or administers funds for designated individuals or entities. The obligation by FIs, DNFBPs, and VASPs to freeze funds of designated individuals or entities applies immediately after a designation is published by the UAE Cabinet on the Local Terrorist List or by the UNSC in its Consolidated List.

Failure by an FI, DNFBP, or VASP to apply freezing measures, immediately or in any case within 24 hours after a designation has been made, or otherwise provide funds or services to or for the benefit of a designated individual or legal entity, constitutes a breach of UAE law and may result in the application of both financial sanctions and imprisonment as set out in the Cabinet Decision.

Some FIs, DNFBPs, and VASPs rely on externally provided screening services (e.g., World Check) and other providers to verify that their clients are not subject to any sanctions. It is important to note in this regard that such online services are useful but should not be viewed as an absolute guarantee of compliance with the obligations under the Cabinet Decision. Additional periodic checks against the designations made in the Sanctions Lists must be carried out.

25. When and how often do I have to conduct screening?

FIs, DNFBPs, and VASPs must undertake regular and ongoing screening on the latest Local Terrorist List and UN Consolidated List. Screening must be undertaken in the following circumstances:

- a. Upon any updates to the Local Terrorist List or UN Consolidated List. In such cases, screening must be conducted immediately and without delay to ensure compliance with implementing freezing measures without delay (within 24 hours).
- b. Prior to onboarding new customers.
- c. Upon KYC reviews or changes to a customer's information.
- d. Before processing any transaction.

FIs, DNFBPs, and VASPs are also required to identify, assess, monitor, manage and mitigate terrorist and proliferation financing risks, particularly sanctions-related risks. The internal screening process must take into account such a risk assessment. Where there are higher risks, FIs, DNFBPs, and VASPs should take commensurate measures to manage and mitigate the risks, including applying enhanced screening measures. Correspondingly, where the risks are lower, they should ensure that the screening measures are commensurate with the lower level of risk. **FIs, DNFBPs, and VASPs must ensure full implementation of targeted financial sanctions in any risk scenario.**

26. How long do I have to keep funds frozen?

The Cabinet Decision does not limit the timeframe for any given freezing measure. Accordingly, the obligation to keep funds frozen could apply indefinitely in some cases.

FIs, DNFBPs, and VASPs are required to lift the freezing measures if the name of a designated individual or entity is removed from the Sanctions Lists.

27. What shall I do if my name is similar to a designated person?

In case freezing measures were taken in relation to funds of a person that has the same (or similar) name as a designated individual or entity but who is in fact not the same person, such person can send a request to lift the freezing measures to the Executive Office.

Such a request should include a grievance letter addressed to the Executive Office of Committee for Goods & Materials Subjected to Import & Export Control and other supporting documents (such as ID documents) and should be sent to the Executive Office by email through iec@uaeiec.gov.ae

28. Is my Supervisory Authority going to check compliance with the Cabinet Decision in the course of their onsite inspections?

The Cabinet Decision No. 74 of 2020 provides that FIs, DNFBPs, and VASPs are under an obligation to have in place adequate processes, policies and procedures, including resourcing thereof, to verify that they are complying with all aspects of the relevant Cabinet Decisions. Supervisory Authorities will verify compliance by FIs, DNFBPs, and VASPs with this obligation during their supervisory activities. A failure to have in place such procedures may result in the application of criminal as well as supervisory sanctions as stipulated in the Cabinet Decision.

29. Are Politically Exposed Persons (PEPs) part of the scope of implementing targeted financial sanctions (TFS)?

No. Obligations to implement TFS are exclusively on the individuals, entities, and groups that are designated on the Sanctions Lists (regardless of whether they are considered as PEPs).

30. Should we conduct screening for Politically Exposed Persons (PEPs)?

PEPs are out of the scope of Cabinet Decision No. 74 of 2020 and you are advised to follow your Supervisory Authority guidance and other best practices on the customer due diligence required when dealing with PEPs, including on screening.

31. Is notifying the customer after implementing freezing measures considered as “tipping off”?

No. FIs, DNFBPs, and VASPs may notify their customers after the freezing measures have been implemented. As long as the customer is notified after the freezing measures have been taken, it is not considered as tipping off.

However, FIs, DNFBPs, and VASPs must not inform their customers prior to taking the freezing measures.

32. What should I do if one of my customers is affected by a freezing measure?

You should notify the customer of the Grievances and Requests process as reflected on the Executive Office’s website.

Annex B: EO Notification / Alert System Subscription Guide

Simple Guide to ***Subscribe to Sanctions Lists***

Introduction

The UAE recognizes two Sanctions Lists:

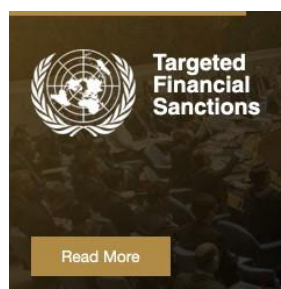
- The UAE Local Terrorist List - issued by the UAE Federal Cabinet
- The United Nations Consolidated List - issued by the United Nation Security Council

Both Lists Are Being Updated Periodically By The Issuing Authorities

Accessing the Lists

The United Nation Consolidated List and UAE Local Terrorist List can be accessed from the Executive Office's website <https://www.uaieic.gov.ae/en-us/un-page>

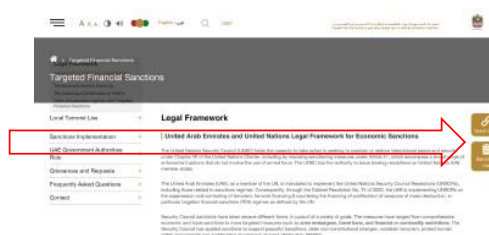
To receive updates on both Sanctions Lists, please subscribe to the Executive Office mailing list



Subscribe to the Sanctions List (1/3)

Step-1: Access the following link <https://www.uaieic.gov.ae/en-us/un-page>

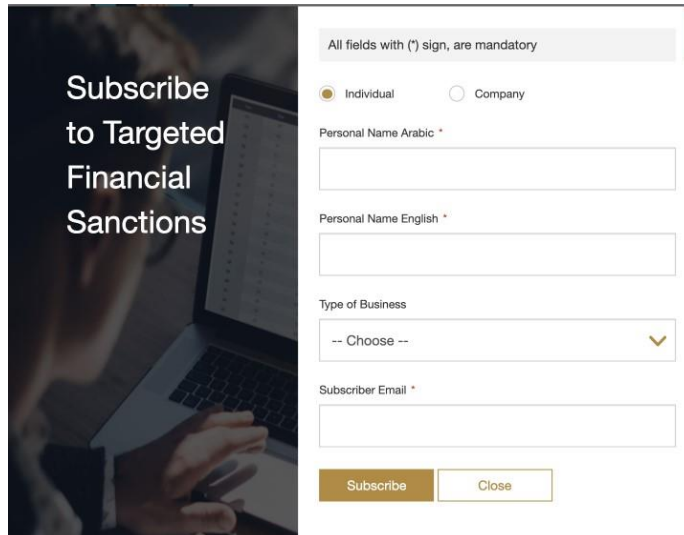
Step-2: Navigate to "Sanction List" in the quick links section



Step-3: Click on Subscribe

Subscribe to the Sanctions Lists (2/3):

- **Step-4:** Fill the Form



Subscribe to Targeted Financial Sanctions

All fields with (*) sign, are mandatory

☒ Individual ☐ Company

Personal Name Arabic *

Personal Name English *

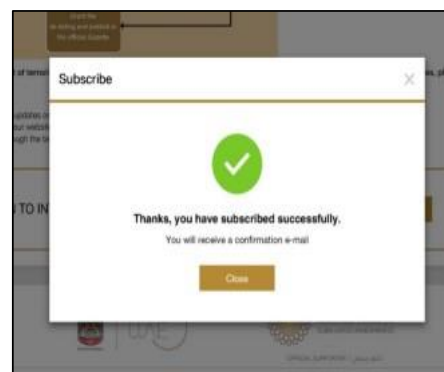
Type of Business
-- Choose --

Subscriber Email *

Subscribe Close

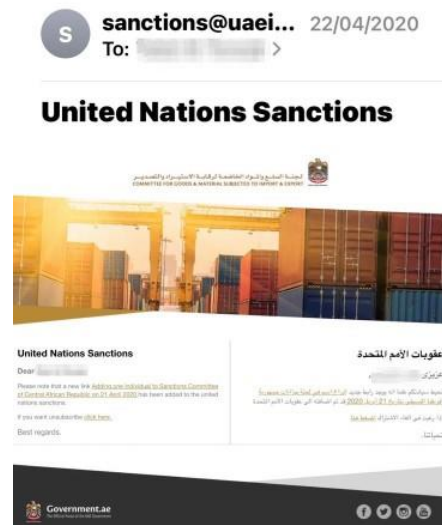
Subscribe to the Sanctions Lists (3/3):

- **Step-5:** Submit the information by clicking “**Subscribe**”. Subscribers will receive a confirmation email automatically after the subscription.



Update Notification

- Upon any update on the UAE Local Terrorist List or the UN Consolidated List, all users will receive a notification of the update through email



Document Version Update

Date	Section	Update
07 Nov 2021	Full Document	Updated to include Virtual Asset Service Providers (VASPs)
	Section 1	Updated legal framework to include Federal Decree No. 26 of 2021 Amending Certain Provisions of Law No. 20 for 2018 on Anti-Money Laundering and Countering the Financing of Terrorism
	Section 3	Revised definition of “funds or other assets” as per FATF Standards
	Section 4	<ul style="list-style-type: none"> Updated definition on ‘confirmed match’, ‘potential match’, and ‘false positive’ Updated TFS screening and reporting procedures
	Section 5	Revised section on ownership, control, and acting on behalf or at the direction of
	Section 6	Enforcement updated as per Article 28 of Federal Decree No. 26 of 2021
	Section 10	Updated procedure for submitting de-listing request from UN List
	Annex A	Updated FAQs
	Annex B	Added EO Notification System Subscription Guide

Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction

United Arab Emirates

Issued by the Executive Office of the Committee for Goods
Subject to Import and Export Control

© Executive Office of the Committee for Goods Subject to
Important and Export Control, 2021

<https://www.uaieec.gov.ae/en-us/>

Email: iec@uaieec.gov.ae

Issued on: 20 Mar 2021

Last amended: 14 Nov 2021

Acronyms

CBUAE	Central Bank of United Arab Emirates
DPRK	Democratic People's Republic of Korea
Executive Office or EO	The Executive Office of the Committee for Goods & Materials Subjected to Import & Export Control
FATF	Financial Action Task Force
FANR	Federal Authority for Nuclear Regulation
FCA	Federal Customs Authority
FIU	Financial Intelligence Unit
ISIL	Islamic State in Iraq and the Levant (Da'esh)
PF	Proliferation Financing
TF	Terrorist Financing
UAE	United Arab Emirates
UN	United Nations
UN Panel of experts	The Panel of Experts pursuant to UNSCR 1874 related to the Nuclear Programme of the Democratic People's Republic of Korea
UNSC	United Nations Security Council

UNSCR	United Nations Security Council Resolution
US	United States of America
WMD	Weapon of Mass Destruction

Contents

Acronyms.....	1
Introduction.....	5
Targeted Financial Sanctions related to Terrorism and Terrorist Financing.....	6
Banking Services.....	7
Money Remitters	8
Exchange Houses	8
Hawala and Other Similar Service Providers (HOSSP)	9
Online Payment Facilities	10
The Misuse of Non-Profit Organizations (NPOs)	12
Support for Recruitment of Foreign Terrorist Fighters.....	12
NPO Affiliation with a Terrorist Entity	13
Donations to NPOs Affiliated with Terrorist Groups.....	14
Cash Smuggling	14
Smuggling of Gold.....	15
Circumventing Sanctions Through Trade.....	16
Trade In Dual-Use Goods	16
Trade of Communication Devices.....	17
Trade of Natural Resources.....	17
Trade of Oil and Derivates	17
Trade of Charcoal from Somalia	18
The Misuse of Legal Entities	18
The Use of Virtual Assets to Support TF Groups.....	20
Transferring funds via Bitcoin	20
Use of Virtual Assets Ethnically or Racially Motivated Terrorist Financing	20
Promotion of virtual currency to fund terrorism.....	20
Targeted Financial Sanctions Related to Proliferation of WMD.....	22
The use of Banking Sector	23
Designated banks maintain representative offices and agents abroad	23
Financial activities of diplomatic and other personnel of the DPRK.....	24
Transfers through banks	24
Use of cash to circumvent US sanctions	25
Cyberactivity targeting financial institutions	25
Operation "FASTCash".....	26

Cyberattack on Cryptocurrency Exchange House	27
Economic Resources.....	27
Oil Ship-To-Ship Transfers	28
Smuggling Petrochemicals	28
Nickel Wire	28
Carbon Fiber	29
Trade-In Other Goods	29
Generator.....	29
Vibration Analysis Devices.....	30
Misuse of Legal Entities or Arrangements.....	31
Purchasing Aircraft Equipment Through 3rd Party	31
DGS Marine.....	31
The GENCO/KOGEN Group	32
GENCO Network	34
The Glocom Group.....	34
Financial Operations Of Glocom/Pan Systems Pyongyang	35
TFS - TF Red Flags	37
TFS – PF Red Flags	39
References	42
Document Change Log	45

Introduction

The United Nations Security Council (UNSC), pursuant to Chapter VII of the United Nations Charter with the aim to maintain peace and security through its Resolutions and Sanctions Committees, mandates the implementation of various sanctions regimes. This document is focused mainly on the UNSC sanctions regimes, particularly, those related to non-proliferation of weapons of mass destruction, terrorism, and their financing.

The term *Targeted Financial Sanctions (TFS)* includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of individuals, entities, groups, or organization who are designated pursuant to the UNSCRs and Local Terrorist List. In particular, the UNSC has imposed targeted financial sanctions on individual, entities and group considered global terrorists, and to the nuclear programs of Iran and DPRK.

This document presents cases and examples from the UAE and other countries on how these sanctioned activities, persons, groups, or entities have received financing and support, therefore in violation or evading UNSC Resolutions (UNSCR) in particular the ones related to UNSCR 1267 (1999), 1989 (2011), 1988 (2011), 1718 (2006), 2231 (2015) and their successor resolutions. This document also presents cases related to the national UAE terrorist list in accordance with UNSCR 1373.

This document also includes a list of red-flags and indicators that help the financial institutions (FIs) and Designated non-financial businesses and Professions (DNFBPs) to detect any suspicious transactions related to Terrorist Financing (TF) and Proliferation Financing (PF).

All information presented in this document derives from public sources and guidelines issued by FATF. It includes a compilation of UAE and international case studies aiming to provide trends and methods used by sanctioned persons, groups, or entities to circumvent the UNSCR. The government authorities and private institutions to ensure full implementation of TFS requirements, effectively preventing the breach, non-implementation or evasion of TFS.

Targeted Financial Sanctions related to Terrorism and Terrorist Financing

The term terrorist financing includes the provision of funds or assets to commit terrorist activities. This term includes providing food, lodging, training, and making means available such as transportation and communication equipment. Such financing can occur with money or in kind, and funds involved can be from legal or illegal sources. The targeted financial sanctions aim to prevent the financing of terrorists.

The following are methods and cases that illustrate how terrorist groups have misused economic sectors or activities to fund their activities, in breach of sanctions. 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

In its report "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)" of 2015, FATF identified that this terrorist organization earns revenue primarily from five sources: (1) 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; (2) kidnapping for ransom; (3) donations including by or through non-profit organizations; (4) material support such as support associated with foreign terrorists fighters and (5) fundraising through modern communication networks¹.

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), of 3 June of 2020 ("Joint Report") concludes from a questionnaire sent to all United Nations Member States that the most frequently used channels for terrorist financing are (1) the formal banking system; (2) cash smuggling; (3) the money services business; and (4) informal remitters or hawala².

The Joint Report also accounts for the abuse of technology (including social media, prepaid cards, and mobile banking) for terrorist purposes, noting that terrorist financing was facilitated by recent developments in mobile payments and the anonymity of money transfers and illicit donations via crowdfunding platforms.³

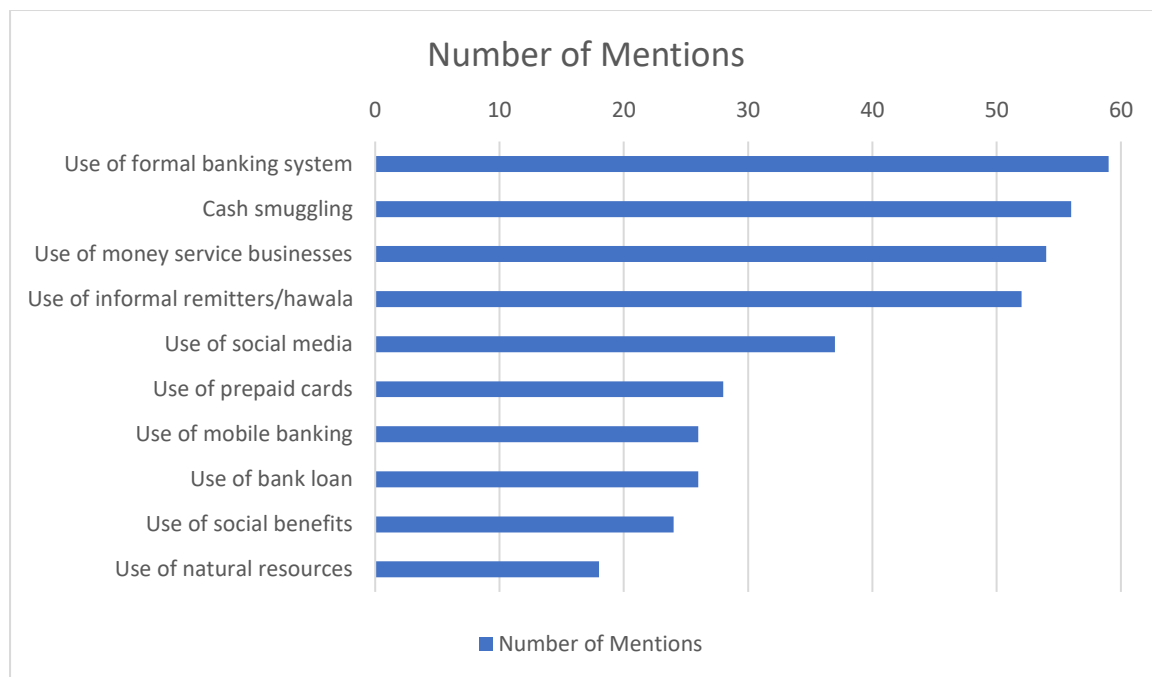
¹ Financial Action Task Force, 2015, p. 12

² United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 16.

³ United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 17.

The UNSC notes that terrorists and terrorist groups raise funds through various means, including exploiting natural resources, kidnapping for ransom, and links to organized crime and drug trafficking. The Joint Report notes the potential for terrorism financing through the construction and real estate sectors, the use of shell companies to conceal cash, the use of non-profit organizations, and trade-based terrorism financing.⁴

Figure-1: Methods most frequently used by terrorist financiers



Source: United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), S/2020/493, p. 16.

Banking Services

The formal banking system is vulnerable to the circumvention of sanctions related terrorist financing because all financial product and services, could be misused or vulnerated to finance terrorism, in addition to the difficulty of distinguishing between legitimate and illegitimate low-cost transactions and detecting indirect transactions. Unfortunately, transaction-monitoring programs are often unable to identify terrorism financing.⁵

⁴ United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 17.

⁵ United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015) , S/2020/493, p. 16.

Continued access to bank accounts by foreign terrorist fighters

Foreign terrorist fighters are individuals who travel to a states other than their state of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict⁶.

According to financial information, terrorist financing risks were identified when foreign cash withdrawals via ATMs made in areas located near territories where ISIL operates by unknown individuals. These withdrawals were taken from US-based bank accounts using a debit card. Another terrorist financing risk identified was the existence of large deposits into bank accounts followed by immediate foreign cash withdrawals in areas located near to territories where ISIL operates. This information reveals the terrorism financing risks posed by the ability of the individuals who are believed to have travelled to areas occupied by ISIL to reach their bank accounts in their home countries.⁷

Money Remitters

Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to Terrorist Financing. 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 activity. Remittance providers are especially vulnerable to abuse by Terrorist Financing where they are unregulated, not subject to appropriate AML/CFT supervision, or where they operate without a license (thus working without any AML/CFT controls)⁸.

Exchange Houses

The UAE authorities arrested a person for transferring money to a jihadist group in the Philippines who pledged allegiance to ISIL terrorist organization. The suspect received money from persons from different places in the UAE using Exchange House. The money was sent through multiple payments and in small amounts so that the UAE authorities would not identify them. The investigation determined that the transferred funds' total value accounted for AED 120,000 (USD 32,671).

⁶ Security Council resolution 2178 (2014) S/RES/2178

⁷ Financial Action Task Force, February 2015, p. 23

⁸ Financial Action Task Force, October 2015, p.26

Hawala and Other Similar Service Providers (HOSSP)

There are several reasons why HOSSPs poses a terrorist financing vulnerability, including a lack of registration and supervision, settlement across multiple jurisdictions through value or cash outside of the banking system, the use of businesses that are not regulated financial institutions, the use of net settlement and the commingling of licit and illicit proceeds⁹.

Funds Sent to Boko Haram

The UAE authorities received information from secret sources and LEA intelligence on six individuals of Nigerian nationality suspected of financing Boko Haram, a terrorist group designated in the UAE Local Terrorist List and UN List (UNSCR 1989), by transporting and transferring funds from the UAE to the terrorist group. The suspects conducted large transfers which were not commensurate with their income from their jobs in the UAE.

The investigation found that the suspects received the funds in cash (Nigerian Naira) in Nigeria and transported the cash physically to the UAE. The funds were concealed and their source disguised when entering the UAE. Once in the UAE, some of the funds were exchanged for U.S. dollars then re-exchanged to Naira and physically transported back to Nigeria, while other funds were transferred back to Nigeria through exchange houses in which some of the suspects were employed. These funds were from illegal sources and included funds stolen from the Nigerian government.

In April 2017, law enforcement authorities arrested the suspects and seized AED 3,000,000 in cash and instrumentalities worth AED 40,000 in the possession of the suspects. The Prosecution issued a freeze order on cash (AED 3,000,000) and instrumentalities (AED 40,000). The six suspects were prosecuted and convicted of TF (and other offenses). In 2019, the court sentenced two defendants to life imprisonment and four defendants to imprisonment for ten years followed by deportation. The court also confiscated the full value of cash and instrumentalities seized and frozen.

Funds Sent to ISIL In Afghanistan

The UAE authorities arrested nine (9) persons who were members of the ISIL terrorist organization that received military training on the use of weapons in Khorasan, Afghanistan. The suspects were involved in moving, transferring, and sending funds through a Hawala Service provider using tailor shops. They were also exchanging the currency into US dollars and handing it over to persons with Afghan nationalities for them to send them to Afghanistan. The transferred funds' value reached AED 243,410 (USD 66,270).

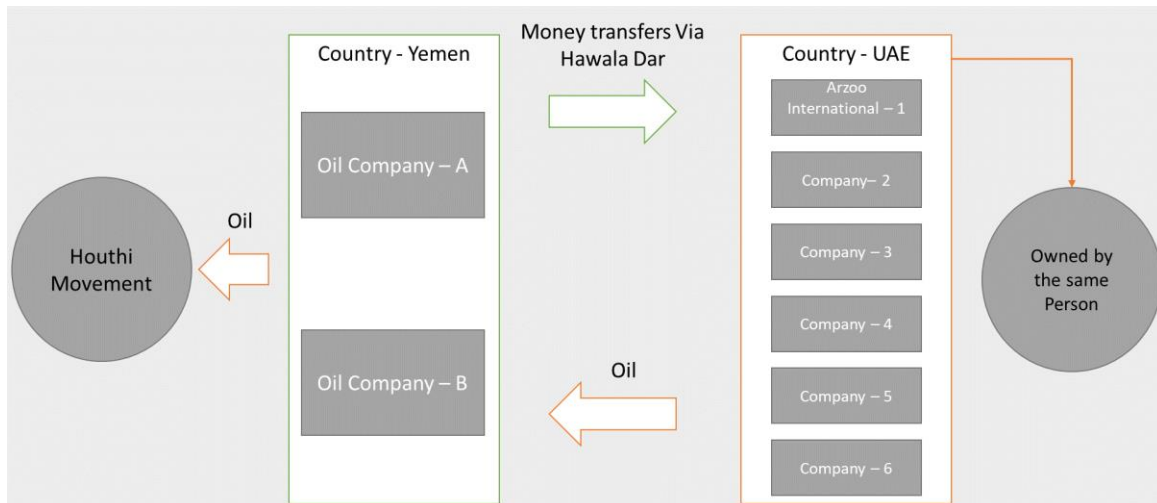
⁹ Financial Action Task Force, October 2013, p. 41

Funds Sent to Houthies In Yemen

The UAE authorities received intelligence showing high volume money transfers sent via Hawala from two oil companies based in Yemen to six entities based in the UAE. The six entities shared the same beneficial owner, and one of the entities (Company A) was mentioned in an official communication (OC) received by the UAE from the UN Yemen Panel of Experts. Shortly thereafter, the beneficial owner of the six companies transferred the financial activities of the six entities to a new entity (Company B), also based in the UAE, and appointed a nominee as the owner of Company B to hide the beneficial ownership details.

Initial investigations uncovered that the originators of the transactions were two Houthi-owned oil companies. (The Houthi Movement in Yemen is designated in the Local Terrorist List pursuant to Cabinet Decision No. 41 of 2014.) The State Security Prosecution issued freeze orders on the assets of the involved persons and entities and their bank accounts with a total amount of AED 54 million. Five main suspects were detained and interrogated, one of whom was the beneficial owner of the six entities mentioned above.

The UAE Authorities also took the decision to suspend the trade licenses of the companies involved, and one of the companies (H F Z A ARZOO INTERNATIONAL FZE) was designated on the Local Terrorist List based on Cabinet Resolution No. 83 of 2021.



Online Payment Facilities

Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Funds

transfers are often made by electronic wire transfer, credit card, or alternate online payment facilities.¹⁰

Online payment facilities can be vulnerable to identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes, and auction fraud. The following cases illustrate how online payment facilities are vulnerable to circumvent sanctions related to terrorism.

Fundraising Through the Internet

Information obtained by way of Intelligence indicated that some individuals associated with ISIL have called for donations via social media and have asked the donors to contact them through online communication tools. 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 online communication tools. The fundraiser would then send the number to one of his followers in a close country from Syria and sell the card number at a lower price and take the cash that was afterward provided to ISIL¹¹.

Online Financial Accounts Used for Fundraising

The United Kingdom case against Younis Tsouli: Profits from stolen credit cards were laundered by several means, including transfer through e-gold online payment accounts, which 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 Tsouli 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 approximately £1.6 million of illicit funds to finance terrorist activity¹².

The Use of Social Media and Telegram Platforms to Promote Terrorist Activities

- The UAE authorities investigated persons who adopted terrorist and extremist ideas. They use information technology to explore methods to organize terrorist organizations and send money to terrorists and ISIL. One of the suspects, adopting the ideology of ISIL, was caught communicating with terrorist persons from abroad using Social Media platforms. He had also exchanged videos and photos endearing and promoting ISIL and transferred these clips to colleagues for

¹⁰ United Nations Office on Drugs and Crime, 2012, p. 7

¹¹ Financial Action Task Force, February 2015, pp. 24-25

¹² United Nations Office on Drugs and Crime, 2012, p. 7

promotion. Also, through his communication via social media, he communicated with a person from outside the UAE who requested financial assistance to join the ISIL. The suspect sent an amount of money to help this other person join ISIL through an Exchange house, and he had also provided an amount of money to two (2) of his colleagues to help them prepare for travel so that they could join the ISIL.

- A person was arrested in the UAE for aiding Al-Nusra and its affiliated groups in Syria, by providing them logistical. The suspect also supported the fighters in the Turkmen Brigade in Syria and provided transportation to country X border. He confessed that he used his account on one of the social networking platforms to collect assistance and fundraise to support Al-Nusra and the armed brigades in Syria. Also, used a telegram platform to promote terrorist organizations by publishing videos and pictures endearing and promoting the organizations. The value of the money raised was approximately AED 312,000.
- Based on an investigation carried out by the UAE authorities, it was identified that there are group of people residing in the UAE who support ISIL by using various means. Accordingly, a person of Syrian nationality was arrested for facilitating the transfer of funds in favour of members of the Al-Nusra organization. The suspect used one of the social networking platforms to tell a friend about the location of the money and requested him to send it through an exchange house to another person who is in country X, who is a member of the Al-Nusra Front. The amounts of money that he transferred accumulated to AED 10,000.

The Misuse of Non-Profit Organizations (NPOs)

Individuals and organizations seeking to fundraise for terrorism and extremism support may attempt to disguise their activities by claiming to be engaged in legitimate charitable or humanitarian activities. They may establish NPOs for these purposes¹³. The following cases illustrate how NPOs are vulnerable to be misused to circumvent sanctions related to Terrorism.

Support for Recruitment of Foreign Terrorist Fighters

On 4 November 2010, 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, including al Qaida and affiliated organizations.

Al Rehmat Trust was found to be serving as a front to facilitate efforts and fundraising for an UN-designated terrorist organization, Jaish-e Mohammed (JEM). After it was banned in Pakistan in 2002, JEM, a UN 1267 designated Pakistan-based terrorist group, began using Al Rehmat Trust as a front for its operations. Al Rehmat Trust has

¹³ Financial Action Task Force, October 2015, p. 32

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. 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.

Al Rehmat Trust has also provided financial support and other services to the Taliban, including financial support to Afghanistan's wounded Taliban fighters¹⁴.

NPO Affiliation with a Terrorist Entity

In August 2013, the US Department of the Treasury designated the Jamia Taleem-UI-Quran-Wal-Hadith Madrassa, also known as the Ganj Madrassa, pursuant to US Executive Order (EO) 13224 for being controlled by, acting on behalf of, and providing financial support to al-Qa'ida and other designated terrorist organizations. The Ganj Madrassa is a school in Peshawar, Pakistan, that was found to be serving as a training centre for and facilitating funding for UN and U.S.-designated terrorist organizations, including al-Qa'ida, Lashkar-e Tayyiba, and the Taliban. The activities of the Ganj Madrassa exemplify how terrorist groups, such as al-Qa'ida, Lashkar-e Tayyiba, and the Taliban, subvert seemingly legitimate institutions, such as religious schools, to raise and divert charitable donations meant for education to support terrorist training and violent acts. The action did not target all madrassas, which often play an essential role in improving literacy and providing humanitarian and developmental aid in many areas of the world; it only identified this specific madrassa as supporting terrorism and terrorist financing.

The Ganj Madrassa is controlled by UN-designated al-Qa'ida facilitator Fazeel-A-Tul Shaykh Abu Mohammed Ameen Al-Peshawari, also known as Shaykh Aminullah. Shaykh Aminullah was designated by both the United States pursuant to US Executive Order (EO) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organizations and the United Nations (UN) in 2009 for providing material support to al-Qa'ida and the Taliban.

The Ganj Madrassa serves as a terrorist training centre where students have been trained to conduct terrorist and insurgent activities under the guise of religious studies. In some cases, students were trained to become bomb manufacturers and suicide bombers. Shaykh Aminullah has directed donations provided for the school to terrorist groups such as the Taliban, which use the money to fund the ongoing violence in Afghanistan¹⁵.

¹⁴ Financial Action Task Force, June 2014, p. 46

¹⁵ Financial Action Task Force, June 2014, p. 117

Donations to NPOs Affiliated with Terrorist Groups

- On 11 October 2020, a local bank froze and raised a notification to the Central Bank that Company X sent a wire transfer “donation” of GBP 5,000 (AED 25,000) to a beneficiary located in Country A. The notification mentioned that the recipient was identified as “Islamic Relief”, which is a name similar to a listed designation in the UAE Local Terrorist List pursuant to Cabinet Decision No 41 to 2014.

The UAE authorities reviewed Company X’s criminal records and verified financial transactions and any related information or documents. The investigation remains ongoing towards Company X; however, the Person was clear of any criminal records or suspicious activities. The UAE authorities took preventative measures towards the designated entity's website being banned to prevent further donations.

- On 31 August 2021, a local bank raised a Partial Name Match Report (PNMR) via GoAML. The bank identified (through open-source information) a business relationship between a customer (regional bank) and the Islamic Relief Worldwide (IRW), which is registered as a charity and supervised by Country A.

According to Cabinet Decision 74 to 2020, the bank took immediate action in freezing the accounts without delay and informed the Executive Office – IEC and Supervisory Authority with all relevant information.

Cash Smuggling

Cash continues to be a prevalent aspect of terrorist operations. While funds may be raised in several ways, they are often converted into cash to be 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 economies¹⁶. The following cases illustrate how smuggling is used to circumvent sanction on Terrorism.

The UAE authorities arrested a person involved in providing Yemen's Houthi Terrorist Movement with funds and assistance by sending funds estimated at AED 200,000 with a driver who transported such cash across the land borders.

¹⁶ Financial Action Task Force, October 2015, p. 23

Smuggling of Gold

The UAE authorities provided intelligence to the Federal Customs Authority on an illegal shipment heading from Country X to UAE that belongs to an extremist movement in Country X. The leader of the extremist movement is designated in OFAC. The Federal Customs Authority issued a notice to all local customs to increase the inspection procedures on any shipment being imported from Country X. Local Customs have identified Person S with an illegal shipment coming from Country X. Customs and State Security have conducted a criminal investigation and found that the shipment contains 60 kgs of Gold without proof of origin.

The UAE Prosecution has received all the information related to the investigation and issued an order to arrest Person S and seize the shipment.

The court reviewed the documents based on the investigation reports received from UAE Prosecution and have issued a verdict on Person S to serve a lifetime prison sentence and confiscate the 60 kgs of gold worth AED 6,000,000.

Cash Couriers

Over a period of three consecutive days, three individuals declared a total amount of some EUR 90,000 in cash to customs officials at the airport in Brussels. The funds are said to originate from NPO A from Germany as part of humanitarian aid in Burundi, Benin, and Zimbabwe. The three couriers are all Belgian nationals and have been living in Belgium for a long time. A Belgian coordinating body of a radical Islamic organisation 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 is 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.

According to information from the Belgian intelligence services, the three individuals referenced above are known to be involved in local branches of a radical Islamic organization. Given the nature of the transactions and the links between the two NPO referenced above, Belgian authorities suspect that at least part of the funds described above could have been used to support terrorist activities.¹⁷

¹⁷ Financial Action Task Force, October 2015, p. 23

Circumventing Sanctions Through Trade

Trade can be very vulnerable to circumvent sanctions against terrorism. It is challenging to identify when sanctioned persons are involved in any part of the value of chain of trade. The following cases illustrate how sanctions can be circumvented through trade.

Trade In Dual-Use Goods

- Early 2019, the UAE authorities received intelligence information regarding two business activities, owned by Naif Al Jarmouzi, and supports the Houthi Movement in Yemen, a terrorist group designated in the UAE Local Terrorist List. Moreover, the terrorist group received support through multiple channels such as cash, chemical materials, electronics, electrical generators, solar panels, and telecom gadgets and that was made through forging bills of lading. One hundred tons of chemical items, among them MDA, were identified as being shipped and valued at AED 220,000.

The investigations have identified a total amount of AED 101,000 belonging to the suspect and his companies and were used to support the Houthi Movement in Yemen. Moreover, a report from the customs authorities confirmed that bills of lading were forged.

The UAE Prosecution issued an order to arrest Naif Al Jarmouzi, freeze and confiscate funds and other assets totaling an amount of AED 101,000 and suspend the business activities of Naif Al Jarmouzi's companies.

The UAE Prosecution provided the Supreme Council for National Security with reasonable grounds to designate Naif Al Jarmouzi and his three companies, accordingly, the individual and the two entities were designated in the Local Terrorist List based on Cabinet Decision No. 83 of 2021.

- An informal intelligence information was received by UAE authorities about a shipment transported as a transit. The shipment contained a chemical component listed as a dual-use item. After investigation, the UAE authorities identified that the beneficiary of this shipment is the "Somali Youth Movement", which is designated in the UAE Local Terrorist List and UNSCR 1267 list.

The UAE Prosecution confirmed, with the support of experts, that the shipment material is Potassium Nitrate, an item listed as an explosive precursor according to paragraph (28) of UNSCR 2498 (2019). The shipment included four containers worth a value of AED 247,000. The UAE Prosecution issued an order to seize and restrain the shipment in coordination with federal customs and relevant port authorities.

Trade of Communication Devices

A Yemeni national supplied Yemen's Houthi Terrorist Movement with funds, means of communication, tools, and chemicals through a shipping company. The suspect has carried out several equipment smuggling operations to Yemen through a company in the UAE with the support of a third suspect. These suspects smuggle a consignment of servers and communication devices belonging to Telecom Company (six (6) wooden boxes containing servers - a large number of small cartons in it containing small black devices) in favour of the Houthis in Yemen for an amount of USD 13,000. To smuggle them, the suspect tore down the papers affixed indicating that these were communication devices and dyed the Telecom Company logo attached on the wooden boxes with a black dye to cover them up and not allow them to be identified. A third suspect produced and forged bills of lading with different data for the shipped devices. They were recorded in the bill of lading as computers and automobile spare parts. The aim was to facilitate importing and smuggling from one of the land border crossings in the UAE due to the prohibition to export them into Yemen. The first suspect also smuggled communication equipment, SIM cards, generators, and chemicals in favour of the Houthis.

In another similar case, another person was arrested by the UAE authorities for shipping auto spare parts and pipes, as well as wired and wireless devices (walkie-talkies) based on instructions from Houthi leaders.

Trade of Natural Resources

The targeted financial sanctions imposed by the United Nations include the freezing and prohibition to provide economic resources, including natural resources to terrorists. The following are cases that show how there was an attempt to circumvent sanctions, but UAE authorities were able to prevent these resources to reach terrorists.

Trade of Oil and Derivates

UAE authorities arrested a person for supplying Yemen's Houthi Terrorist Movement with funds and Iranian diesel. The diesel was smuggled through maritime routes from country X to the Port of Al-Hudaydah in Yemen. The diesel was sold to entities affiliated with Yemen's Houthi Terrorist Movement through three (3) companies owned by the suspect that operate in the oil business. The value of the companies in Yemen is estimated at AED 255,000,000 (USD 69,426,000).

Trade of Charcoal from Somalia

Based on UN resolution no (2036) in 2012 regarding the ban of charcoal from Somalia due to using charcoal revenue to financing Alshabab terrorist group, FCA, Local Customs and the EO has ban importing charcoal from Somalia and monitor the trade and market for diversion of the goods. The following is the investigation findings:

1. Somalin Charcoal has diverted to several country such as Comoros and Iran
2. Counterfeited Certified of Origin
3. Counterfeited bill of Lading

UAE authorities seized the Charcoal and sold it in auctions.

The Misuse of Legal Entities

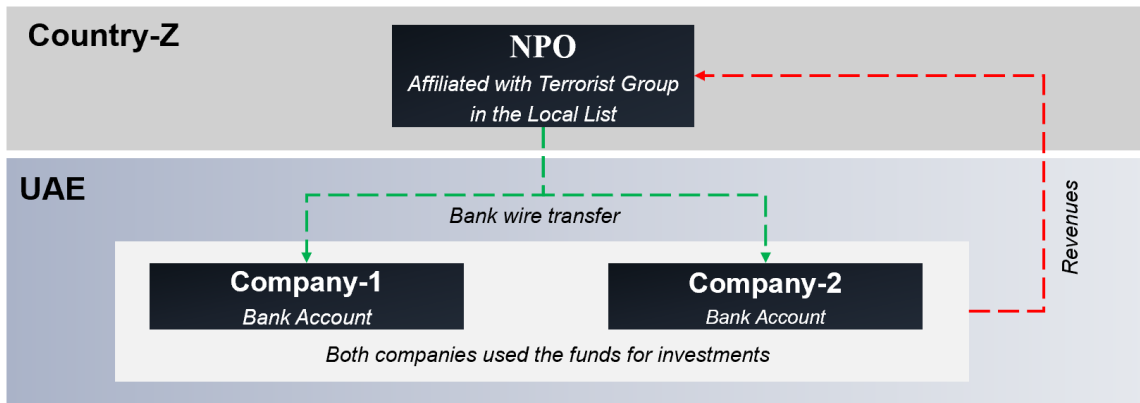
Legal entities can be misused to circumvent sanctions by means of the characteristics of the legal type of entity, for example by using a legal entity as a shell company, or complex legal structures to obscure the beneficial owner. Another method is through the misuse of the economic activity developed by the legal entity. Trade and commercial activities are among the highly vulnerable activities for sanctions evasion related to terrorism. The following case illustrate how legal entities in the UAE can be misused to circumvent sanctions.

- A local bank submitted an STR to the FIU related to domestic legal persons, NYBI Trading and KCL General Trading. Both companies have received funds from foreign NPOs from Country Z which affiliates with the Muslim Brotherhood, a terrorist group listed on the UAE Local Terrorist List.

The UAE authorities found that both companies were had the same beneficial owner (Fadi Kamar) and their income was not consistent with their stated business activity. The investigation found that the companies had transferred a total amount of AED 51 million to different legal persons within the UAE using cheques or cash withdrawals.

The FIU, in cooperation with the Central Bank issued a freezing order for accounts held by the companies in this network. As a result of the order, 49 accounts with a total value of AED 29 million were frozen.

Post investigations, the UAE Prosecution referred 31 individuals and 28 entities to court f. The court issued a verdict to imprison the main suspect (Fadi Kamar) for life and nine other suspects were sentenced to ten years of imprisonment. In addition, the convicts were ordered to pay a penalty of AED 500,000 per person. The court also convicted two entities (NYBI Trading and KCL General Trading) penalizing them with AED 500,000 each and terminating their business licenses. The remaining 21 individuals and 26 entities were declared innocent. The court confiscated a total of AED 20 million related to the convicted persons.



- The UAE authorities received intelligence information from informal sources of Person X who resides in the UAE and has a relation with “Jabhat Al Nusra & Ahrar alsham”, which is designated under the UAE Local Terrorist List and UNSCR 1267 list. Person X established business activities in the UAE to support the designated terrorist group.

The investigations revealed that Person X has three companies that are used to financially support the terrorist organization. In addition, the investigations identified funds and other assets worth AED 5.6 million belonging to Person X.

The UAE Prosecution issued an order to freeze all funds and other assets that belonged to Person X and transferred the case to Court and is pending a verdict.

- The UAE authorities received intelligence identifying four UAE companies related to the Muslim Brotherhood, which is designated on the UAE’s Local Terrorist List. The companies operated in the financial and real estate sectors.

The UAE authorities found that the companies had changed their capital structure and transferred money among their accounts to conceal its original source and invest the money on behalf of the designated group. Two companies had purchased real estate in the UAE with a total amount of AED 150 million. The total assets of the four companies amounted AED 283 million.

In addition to the four companies, nine individuals were found to be affiliated to the designated group.

Nine individuals were arrested, and the licenses of the four companies were deactivated by UAE Prosecution. All assets and bank accounts were frozen for all suspects and the case was transferred to the Court. The Court sentenced each of the nine individuals to ten years in prison, revoked the licenses of the four entities, and confiscated all assets of the four companies, including the real estate, amounting to AED 283 million. The court also assessed penalties of AED 100 million.

The Use of Virtual Assets to Support TF Groups.

Transferring funds via Bitcoin

Financial Investigation into the terror attack perpetrated by the Christchurch Mosque shooter in New Zealand on 15 March 2019 found that he had made multiple donations to ERW entities overseas, including Generation Identitaire in France and Martin Sellner in Austria, referencing 'gift' and 'keep up the good work', as well as that he made use of VAs to transfer funds. He was found to be engaged with 'like-minded' individuals via social media, chatrooms and forums. This case involves spontaneous cooperation after the fact from FIU of the countries involved.

Source: New Zealand ¹⁸.

Use of Virtual Assets Ethnically or Racially Motivated Terrorist Financing

One far-right organization in South Africa created their own stable coin that operates on a 1:1 ratio with the local currency (South African Rand (ZAR)).

The stable coin, managed by an application styled PayApp, enables the group to use digital money as cash. The transactional data lasts 24 hours and thereafter is untraceable.

Bank statement analysis conducted on the accounts of members of the right-wing organization identified specific transactional references used.

The references are in English and or Afrikaans, and include military reference to military ranks, which is indicative of the fact that the group had or has a formal military structure and chain of command.

The Organization raised funds up to ZAR 268,000 (EUR 14,720). ERW actors in South Africa are known to receive financial support from individuals in foreign jurisdictions like the USA, UAE, Australia and Switzerland.

Source: South Africa¹⁹

Promotion of virtual currency to fund terrorism

On 28 August 2015 Ali Shukri Amin was sentenced to 11 years in prison to be followed by a lifetime of supervised release and monitoring of his internet activities for conspiring to provide material support and resources to the ISIL.

¹⁸ FATF report Ethnically or Racially Motivated Terrorism Financing June 2021

¹⁹ FATF report Ethnically or Racially Motivated Terrorism Financing June 2021

Amin pleaded guilty on 11 June 2015. He admitted to using social media platform to provide advice and encouragement to ISIL and its supporters. Amin, who used the social media handle @Amreekiwitness, provided instructions on how to use bitcoin, a virtual currency, to mask the provision of funds to ISIL, as well as facilitation to ISIL supporters seeking to travel to Syria to fight with ISIL.

Additionally, Amin admitted that he facilitated travel for a Virginia teenager, who travelled to Syria to join ISIL in January 2015. This teenager, was charged on 10 June 2015, in the Eastern District of Virginia with conspiring to provide material support to terrorists, conspiring to provide material support to ISIL and conspiring to kill and injure people abroad.

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 this account to conduct conversations on ways to develop financial support for ISIL using on-line currency, such as bitcoin, and ways to establish a secure donation system or fund for ISIL.

For example, Amin shared a link of an article via social media platform he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilise this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which keeps the user of bitcoins anonymous. The article included statements on how to set up an anonymous donation system to send money, using bitcoin, to the mujahedeen.

Source: United States²⁰

²⁰ Emerging Terrorist Financing Risks 2015

Targeted Financial Sanctions Related to Proliferation of WMD

Recommendation 7 of the FATF Standards requires countries to implement proliferation financing-related Targeted Financial Sanctions (TFS) made under United Nations Security Council Resolutions (UNSCRs or resolutions). Recommendation 2 requires countries to put in place effective national cooperation and, where appropriate, coordination mechanisms to combat the financing of proliferation of weapons of mass destruction (WMD). Immediate Outcome 11 and certain elements of Immediate Outcome 1 relating to national cooperation and coordination aim to measure how effective countries are implementing these Recommendations²¹.

The United Nations Security Council (UNSC or UN Security Council) has a two-tiered approach to counter proliferation financing through resolutions made under Chapter VII of the UN Charter and thereby imposing mandatory obligations for UN Member States:

Global Approach Under UNSCR 1540 (2004) and Its Successor Resolutions:

i.e. broad-based provisions both prohibiting the financing of proliferation-related activities by non-state actors and requiring countries to establish, develop, review and maintain appropriate controls on providing funds and services, such as financing, related to the export and trans-shipment of items that would contribute to WMD proliferation. Obligations under the global approach exist separately and do not form part of the FATF Recommendation 7 and its Interpretive Note, and Immediate Outcome 11, but do form part of the FATF Recommendation 2 and are relevant in the context of other FATF requirements on combating terrorist financing and money laundering; and

Country-Specific Approach Under UNSCR 1718 (2006) And UNSCR 2231 (2015) And Their (Future) Successor Resolutions:

i.e., country-specific resolutions against the Democratic People's Republic of Korea (DPRK) and the Islamic Republic of Iran (Iran). The scope and nature of DPRK-related sanctions have been expanded following the country's repeated violations of UN resolutions. On the other hand, UNSCR 2231 (2015), endorsing the Joint Comprehensive Plan of Action (JCPOA), terminated previous provisions of resolutions relating to Iran and WMD proliferation, including UNSCRs 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010), but retained TFS on a number of individuals and entities designated pursuant to these resolutions and also established new specific restrictions, including a number of other measures. TFS obligations under the country-specific approach form part of the FATF Recommendation 7 and Immediate Outcome 11²².

²¹ FATF Guidance on Counter Proliferation Financing 2018

²² FATF Guidance On Counter Proliferation Financing 2018

The term proliferation of weapon of mass destruction (proliferation) does not limit itself to providing or allowing chemical, biological, radiological, or nuclear material or equipment to build weapons, but it also involves the transfer and export of technology, goods, software, services or expertise that could be used in nuclear, chemical or biological weapons-related programs. The targeted financial sanctions aim to prevent the financing of proliferation.

Proliferation financing is providing financial services to those related programs for the transfer and export of nuclear, chemical, or biological weapons, their means of delivery, and related materials. It also involves the financing of trade in sensitive goods needed to support or maintain those programs, even if those goods are not related to any nuclear, chemical, or biological material, such as oil, coal, steel, and military communication equipment. Additionally, proliferation financing includes the financial support to individuals or entities engaged in proliferation, even if they perform other activities that are not related to such programs, such as diplomats, shipping companies, fisheries, and trade-in commodities companies.

The following are cases of violations or evasion of the sanctions imposed by the UNSC related to the Nuclear Programme of the Democratic People's Republic of Korea (DPRK), as presented by the Panel of Experts pursuant to UNSCR 1874, between 2017 and 2020 ("the UN Panel of experts") and the UAE cases related to Proliferation Financing. This paper also gives examples of cases related to the circumvention of the United States of America's sanctions imposed on Iran and the UN sanctions pursuant to UNSCR 1737, continued by UNSCR 2231 related to Iran's nuclear program.

The cases that are explained here involve many sectors, including the financial, trade, and shipping industries. The aim is to increase the awareness in all economic sectors about these sanctions and the importance of their implementation.

The use of Banking Sector

Designated banks maintain representative offices and agents abroad

The UN Panel of experts reported in February 2017 that it had obtained information showing that two UNSC sanctioned banks, Daedong Credit Bank (DCB) and Korea Daesong Bank (KDB), are both operating on Chinese territory, through representative offices in Dalian, Dandong, and Shenyang. A director of such offices also served as a director of a designated company, DCB Finance Ltd., registered in the British Virgin Islands. DCB Finance shared several officers with DCB. When the DCB correspondent accounts were closed in 2005, DCB Finance was set up to undertake wire transfers and business transactions on its behalf²³.

²³ Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 75

The representative in Dalian of DCB and DCB Finance undertook transactions worth millions of United States dollars, including several of \$1 million or more. He also facilitated payments and loans between companies linked to DCB. He exchanged large quantities of bulk cash transferred to China from the DPRK into newer and larger denomination United States dollar notes. He also regularly undertook foreign exchange between United States dollars and euros and transferred balances between DCB and its shareholder, Korea Daesong Bank. When DCB established representative offices in Shenyang in late 2012 and Dandong in 2014, the three offices cooperated in managing the activities of foreign exchange, transfer, bulk cash exchange, and loans²⁴.

In 2019, the UAE expelled representatives of the following DPRK Banks:

- Representative and Deputy representative of Korea Kumgang Group Bank
- A representative of Korea Kumgang Group Bank: Who transported DPRK laborers' money in the Middle East to the DPRK.

Financial activities of diplomatic and other personnel of the DPRK

The UN Panel of experts investigated diplomatic or official personnel of the DPRK who act on behalf of the country's sanctioned financial institutions to establish illicit banking networks and provide the country with access to global banking systems.

The UN Panel of experts investigated reports that Jo Kwang Chol, an accredited member of the administrative and technical staff at the Embassy of the DPRK in Austria since 2016, had engaged in sanctions evasion activities on behalf of the designated Foreign Trade Bank. According to information provided by Austria, Mr. Jo had attempted to gain access to Korea Ungum Corporation's frozen accounts at an Austrian bank. Austrian authorities froze the accounts in July 2015 owing to suspected money-laundering activity. At the time, the total balance was approximately \$1,895,633²⁵.

Transfers through banks

US authorities in 2016 and 2019 indicated the woman, Ma Xiaohong, her company, Dandong Hongxiang Industrial Development Corp., and other executives in the company on charges of money laundering and helping North Korea evade international sanctions.

Before the indictments, Ma and Dandong Hongxiang routed money to North Korea through China, Singapore, Cambodia, the US, and elsewhere, using an array of shell

²⁴ Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 76

²⁵ Report of the Panel of Experts pursuant to UNSCR 1874, S/2020/151, p. 63

companies to move tens of millions of dollars through US banks in New York. There is an estimate that in 2015 there were transfers of US \$85.6 million²⁶.

Use of cash to circumvent US sanctions

The United States and the United Arab Emirates (UAE) jointly took action to disrupt an extensive currency exchange network in Iran and the UAE that has procured and transferred millions in US dollar-denominated bulk cash to Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) to fund its malign activities and regional proxy groups. Specifically, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) designated nine Iranian individuals and entities. Iran's Central Bank was complicit in the IRGC-QF's scheme and actively supported this network's currency conversion and enabled its access to funds that it held in its foreign bank accounts. This network of exchangers and couriers has converted hundreds of millions of dollars²⁷.

Cyberactivity targeting financial institutions

There is evidence that the DPRK, by means of cyberattacks, is stealing funds from financial institutions and cryptocurrency exchanges in different countries, which allows the country to evade financial sanctions and generate income in ways that are harder to trace and subject to less government oversight and regulation. During 2019, there were investigations of at least 35 reported instances of DPRK actors attacking financial institutions, cryptocurrency exchanges, and mining activity designed to earn foreign currency, including in the following Member States: Bangladesh (2 cases), Chile (2), Costa Rica (1), the Gambia (1), Guatemala (1), India (3), Kuwait (1), Liberia (1), Malaysia (1), Malta (1), Nigeria (1), Poland (1), the Republic of Korea (10), Slovenia (1), South Africa (1), Tunisia (1) and Viet Nam (1)²⁸.

According to the UN Panel of Expert, since 2019, there is a marked increase in such cyber activities' scope and sophistication. Some estimates placed the amount illegally acquired by the DPRK at as much as \$2 billion²⁹.

²⁶ NCBC News, 2020, available at <https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329>

²⁷ U.S. Department of Treasury, 2018, [https://home.treasury.gov/news/press-releases/sm0383#:~:text=Washington%20%E2%80%93%20Today%20the%20United%20States,IRGC%20QF\)%20to%20fund%20its,](https://home.treasury.gov/news/press-releases/sm0383#:~:text=Washington%20%E2%80%93%20Today%20the%20United%20States,IRGC%20QF)%20to%20fund%20its,) accessed on February 1, 2021.

²⁸ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26

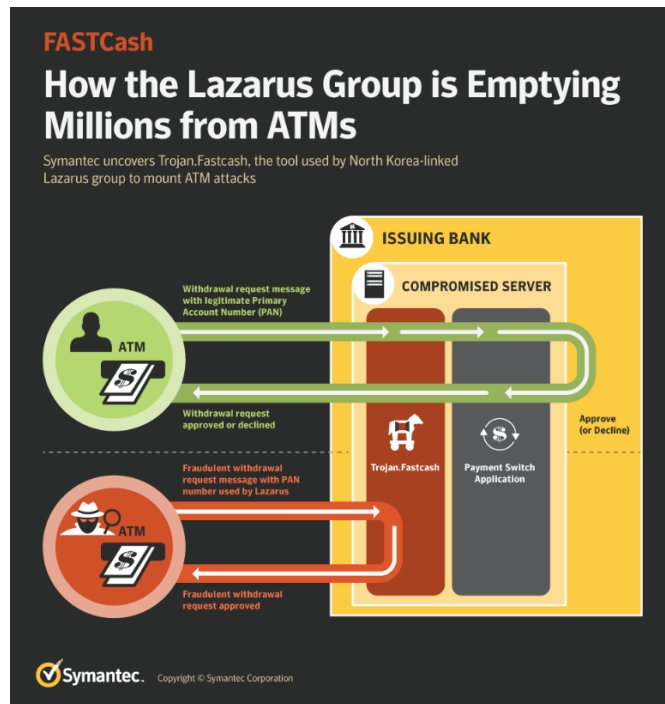
²⁹ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26

Operation "FASTCash"

In its report of August 2019, the UN Panel of experts reported on a cyberattack carried out by DPRK cyber actors who gained access to the infrastructure managing entire automatic teller machine networks of a country. The purposes were to install malware modifying transaction processing in order to force 10,000 cash distributions to individuals working for or on behalf of the DPRK across more than 20 countries in five hours. That operation required large numbers of people on the ground, which suggests extensive coordination with DPRK nationals working abroad and possibly cooperation with organized crime³⁰.

The operation, known as "FASTCash," was enabled by Lazarus, a group involved in both cybercrime and espionage, with apparent links to DPRK. With this operation, it was possible to fraudulently empty ATMs of cash. To make fraudulent withdrawals, Lazarus first breaches targeted banks' networks and compromises the switch application servers handling ATM transactions.

Figure-2: Diagram showing Lazarus Group schemes used to circumvent UN sanctions



Source: "FASTCash: How the Lazarus Group is emptying millions from ATMs," Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

Once these servers are compromised, previously unknown malware (Trojan.Fastcash) was deployed. In turn, this malware intercepts fraudulent Lazarus cash withdrawal requests and sends fake approval responses, allowing the attackers to steal cash from ATMs.

³⁰ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 26

According to a US government alert, one incident in 2017 saw cash withdrawn simultaneously from ATMs in over 30 different countries. In another major incident in 2018, cash was taken from ATMs in 23 separate countries. To date, the Lazarus FASTCash operation is estimated to have stolen tens of millions of dollars³¹.

Cyberattack on Cryptocurrency Exchange House

In 2019, DPRK cyber actors shifted focus to targeting cryptocurrency exchanges. Some cryptocurrency exchanges have been attacked multiple times, in particular those registered in the Republic of Korea. Bithumb was reportedly attacked by DPRK cyber actors at least four times. The first two attacks, in February and July 2017, resulted in losses of approximately \$7 million each, with subsequent attacks in June 2018 and March 2019 resulting in the loss of \$31 million and \$20 million, respectively, showing the increased capacity and determination of DPRK cyber actors. Similarly, Youbit (formerly Yapizon) suffered multiple attacks involving a \$4.8 million loss in April 2017 and then 17 percent of its overall assets in December 2017, forcing the exchange to close³².

Economic Resources

The DPRK uses bulk cash and gold to transfer value by circumventing the formal financial sector entirely. The following are some cases reported by the UN Panel of Experts.

On 6 March 2015, Bangladesh seized 26.7 kg of gold bars and jewellery (worth \$1.4 million) from the hand luggage of the First Secretary of the embassy of the DPRK in Dhaka. An invoice related to those goods had been issued by AMM Middle East General Trading in Dubai, United Arab Emirates, and they were collected from Singapore. The First Secretary had flown into and out of Singapore from Dhaka on the same day, leaving the airport for three hours. He had undertaken on average one such trip per month to Singapore over the previous 15 months from both Dhaka and Beijing (ranging from a few hours to two days on the ground), suggesting that he was serving as a regular diplomatic courier smuggling gold and other items in evasion of sanctions. He was accompanied by other diplomats of the DPRK on some of the trips³³.

On 17 March 2016 in Sri Lanka, an overseas worker of the DPRK was arrested at the airport in Colombo carrying \$167,000 in cash, gold jewellery, and watches. He was in route from Oman to Beijing and made no customs declaration. He was accompanied by five other individuals from the DPRK who were working in Oman for a construction company of the DPRK based in Dubai with a post office box address. He produced a list with 311 names of workers of the DPRK whose families in Pyongyang he was to

³¹ FASTCash: How the Lazarus Group is emptying millions from ATMs, Symantec, 2 October 2018. Available at www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

³² Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 28

³³ Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79

pay (with amounts varying from \$200 to \$1,500, with an average of around \$300 per family)³⁴.

Oil Ship-To-Ship Transfers

Since 2018, the UN Panel of expert's evidence of an increasing frequency of ship-to-ship transfers and one unprecedented prohibited petroleum product transfer comprises 57,623.491 barrels alone, worth \$5,730,886. The Panel's investigation of this transfer reveals a very sophisticated case of DPRK-related vessel identity fraud, highlighting new sanction evasion techniques that defeated the due diligence efforts of the region's leading commodity trader, as well as the United States and Singaporean banks that facilitated the fuel payments and a leading United Kingdom insurer that provided protection and indemnity cover to one of the vessels involved. The case also underlines, once again, the extremely poor reporting, oversight, monitoring, and control over the vessels exercised by the flag-of-convenience States under whose jurisdiction they apparently sail and also the lack of implementation of freezing sanctions³⁵.

Smuggling Petrochemicals

UAE Authorities received intelligence on a maritime business activity that belongs to Person – Z where the leads identify that the person forged shipment policies that belong to Iranian petroleum products being shipped to the UAE from Country – (A).

The UAE authorities found that Person – Z forged the shipment policies to support the Iranian proliferation activities in selling petroleum products and smuggling money to entities based in Iran. In addition, Person – Z assisted Iranian companies in registering the vessels with different country flags to avoid US sanctions.

The UAE Prosecution reviewed the investigation reports, where it issued an order to arrest Person – Z / owner and freeze funds and other assets worth of AED 39,000,000 (USD 10,620,000).

Nickel Wire

In 2019, the UAE authorities received information that Person Z had ties to the Iranian Revolutionary Guards Corps (IRGC) and was involved in financing the nuclear program in Iran in violation of UNSCR 2231. Person Z used the UAE as a transit point

³⁴ Report of the Panel of Experts pursuant to UNSCR 1874, S/2017/150, p. 79

³⁵ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/691, p. 8

for a low-value shipment containing samples of nickel rods/wire which were imported from Country A and destined for Iran.

The UAE authorities identified four bank accounts with a total balance of AED 22,000 that belonged to the suspect and his three companies and were used to support the IRGC. The investigations revealed that Person Z was in negotiations to ship larger quantities of the nickel rods/wire to Iran.

The UAE Prosecution issued an order to arrest Person Z and immediately froze all funds in accounts controlled by Person Z and three companies he controlled, totaling AED 22,000. The UAE Prosecution also suspended the business activity of those companies. The case has been referred to the competent court and is pending a verdict.

Carbon Fiber

In collaboration with the UAE, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) designated 11 entities and individuals involved in procurement on behalf of Iran's ballistic missile program. OFAC sanctioned Mabrooka Trading Co LLC (Mabrooka Trading) – based in the United Arab Emirates (UAE) – and a UAE-based network involved in procuring goods for Iran's ballistic missile program. This network obscured the end user of sensitive goods for missile proliferation by using front companies in third countries to deceive foreign suppliers. It has also designated five Iranian individuals who have worked to procure ballistic missile components for Iran.

Hossein Pournaghshband and his company, Mabrooka Trading, were providing or attempting to provide financial, material, technological, or other support to Navid Composite Material Company (Navid Composite), an entity also sanctioned by the US in connection with Iran's ballistic missile program. At the time of its designation, Navid Composite was contracting with Asia-based entities to procure a carbon fiber production line in order to produce carbon fiber probably suitable for use in ballistic missile components. Since at least early 2015, Pournaghshband used his company, Mabrooka Trading, to procure materials and other equipment for Navid Composite's carbon fiber production plan. Pournaghshband is also designated for having provided or attempting to provide financial, material, technological, or other support to Mabrooka Trading³⁶.

Trade-In Other Goods

Generator

The UAE authorities arrested a man suspected of importing a generator through the company he owned, which operated in the oil and gas business. He imported the

³⁶ U.S. Department of Treasury , 2017, <https://www.treasury.gov/press-center/press-releases/pages/il0322.aspx> accessed on February 1, 2021.

generator from country A, and originally the bill of lading said it was going to be re-exported to country B. But after the device entered the UAE, he forged a bill of lading. He changed the final beneficiary's name from country B to Port of Asalouyeh in Iran, aiming to send the device to Iran's Nuclear Program. The suspect also made financial transfers of the generator's value through his accounts in local banks that were made in batches through the use of a third State, and then transfer the money to a company in country A. The generator was seized, and the suspect was sentenced to ten (10) years imprisonment, deportation, and the confiscation of the device.

Vibration Analysis Devices

- During the permit-approval process, FANR identified a suspicious shipment that contained a dual-use item. Company X, based in a UAE free zone, had submitted three permits to export inverters valued at AED 95,040. The inverters were listed in the UAE Export Control List and classified as a dual-use item. The documents submitted by Company X included a bill of lading and a bill of sales and purchase (BSP), which had conflicting information on the seller's information and the origin country of the shipment. The documents specified that these items were destined for Iran.

The UAE authorities identified that Company X submitted a forged bill of lading, which declared itself as the shipper, while the BSP identified the seller as another company located in Country T. the UAE authorities determined that the purported seller primarily trades in nuts and thus that its business was not consistent with the trade transaction. Further investigations uncovered that the items were in fact imported by the seller from Country H to the UAE. Company X also provided forged documents of having multiple branches in Country U to mislead the authorities and evade sanctions imposed on the Iran nuclear program.

A physical inspection of Company X's premises determined that it was operating as a front for of the buyer of the inverters, located in Iran. The UAE prosecution identified and froze three bank accounts with a total balance of AED 34,000 related to Company X. Furthermore, Customs authorities seized the shipment and State Security Prosecution ordered a freeze on the shipment (AED 95,040).

- In Q2 of 2019, an export application from Company A, based in the UAE, was received by the Executive Office – IEC through the Online Permitting System (OPS) to export an electronic item manufactured in Country B to Iran. The Executive Office – IEC requested more technical details related to the shipment. Company A declared that the item being shipped has a frequency of 599Hz, which is slightly below the threshold for this item to be considered as a dual-use item (600Hz).

The UAE authorities conducted an inspection of the shipment and concluded that Company A provided a false declaration, and the actual technical specification of the item is 650Hz, which is above the dual-use threshold. Subsequently, the EUAE authorities immediately froze the shipment, which was valued at AED 86,000.

The information was shared with the liaison customs officer in Country B to investigate the exporter of the item and validate whether it held a valid license to export such items to Iran. Country B investigated the exporter and its branches and revealed that the exporter did not hold the valid license to export the electronic item and used a general license to circumvent the export system. In addition, Country B seized the electronic equipment and other relevant documents belonging to the exporter and the case was referred to Country B's public prosecution for further investigations.

Misuse of Legal Entities or Arrangements

Purchasing Aircraft Equipment Through 3rd Party

FIU received a suspicious transaction report from a bank in which Person A owns two companies, one of which (Company A) is suspected to purchase aircraft equipment from companies in Country U. The equipment was shipped to Company B, based in the UAE, and working on behalf of an entity listed on the OFAC list that might supports Iranian nuclear program.

The UAE authorities confirmed that Person A and his companies have a business relationship with a listed entity, and the company was used to cover the ultimate beneficiary of the purchased equipment to avoid sanctions. Which a freeze order was issued on his personal and corporate bank accounts.

The UAE Prosecution has confirmed a reasonable ground based on the investigation reports, an order was issued to arrest Person A and freeze the funds and other assets worth AED 4,800,000.

DGS Marine

Until July 2012, DGS Marine was a Liechtenstein-registered offshore business company located at a fiduciary's office in Vaduz. Following June 2012 media reports that DGS's director, David Skinner, had issued insurance certificates for Iranian-owned oil tankers transporting oil from Syria allegedly in contravention of European Union sanctions, the Liechtenstein Financial Authority issued a July 2012 warning notice stating that DGS Marine was not licensed to issue insurance in Liechtenstein. Following the Liechtenstein warning notice, Mr. Skinner registered DGS Marine as a BVI business company in August 2012. The UN Panel of experts was able to confirm that DGS Marine was not licensed or authorized to issue insurance in the BVI either.

In addition, the 2009 DGS Marine annual report contained false information regarding the identity of an individual described as DGS Marine's "independent auditor," calling into question the certification of DGS Marine's annual financial statements. DGS Marine did not respond to the Panel's inquiries, and during the course of the Panel's investigation, the death of Mr. Skinner was announced, and shortly afterward, the DGS website was shut down. Media reporting subsequently indicated that DGS Marine was

an elaborate insurance scam that, while maintaining offices in the United Kingdom, Cyprus, Denmark, Vietnam, India, China, and the United Arab Emirates, did not possess the millions of pounds in securities alleged in its annual reports.³⁷

The GENCO/KOGEN Group

This is a case, published in the UN Panel of experts report pursuant to resolution UNSCR 1874 in March 2019 and August 2019, involving the Korea General Corporation for External Construction (a.k.a. GENCO, a.k.a. KOGEN) group, a network of legal companies and arrangements registered in different countries linked with the Reconnaissance General Bureau, a North Korean intelligence agency that manages the State's clandestine operations.

The UN Panel of experts reported on the ongoing investigation into GENCO/KOGEN that showed that the company has a large reach and extensive network in several countries in the Middle East, Africa, and Eurasia, where it utilizes laborers, prohibited cooperative entities, and joint ventures of the DPRK and earns significant revenue. According to a country, GENCO/KOGEN "has worked to supply North Korean laborers in the Middle East for the purpose of earning hard currency for [the] North Korea [n government]." The Panel's investigations found evidence of KOGEN activity by a joint venture with a company of the United Arab Emirates³⁸.

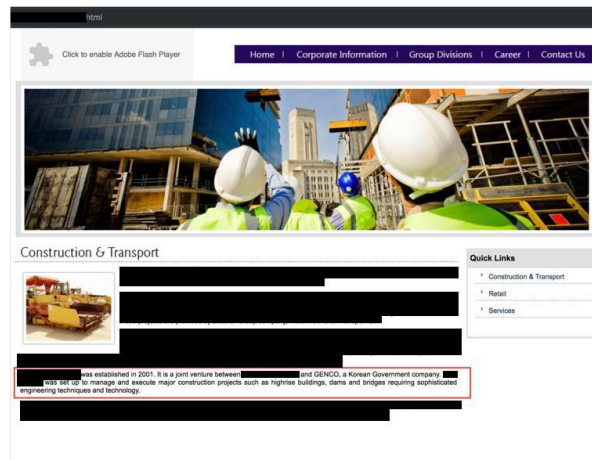
According to corporate registration documents, GENCO is the partial owner of a cooperative construction entity or joint venture company in the Russian Federation, LLC "SAKORENMA," with majority ownership belonging to a Russian national. This cooperative entity or joint venture maintains an account with a Russian bank. Furthermore, the company shares addresses, contact information, and shareholders with three other companies, all of which engage in construction-related activities. In addition, corporate registry documents show that GENCO operates two official representative offices in the Russian Federation, one in Vladivostok and one in Khasan, that together formally employ 17 foreign nationals.³⁹

³⁷ Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 206

³⁸ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56

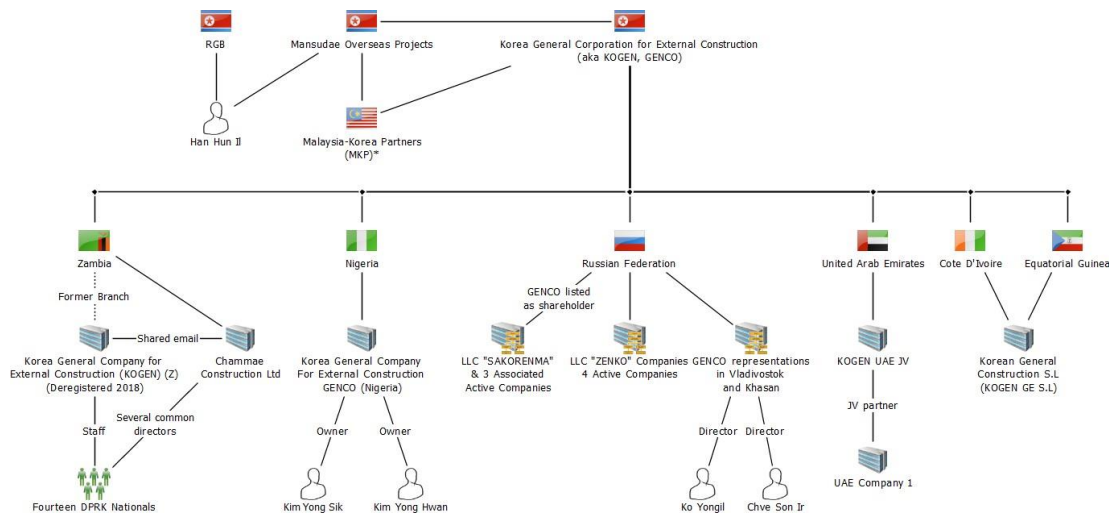
³⁹ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56

Figure-3: Website of KOGEN entity in the United Arab Emirates



The presence of GENCO/KOGEN in Africa covers Nigeria, Côte d'Ivoire, and Equatorial Guinea. In Nigeria, it is registered as "Korea General Company for External Construction GENCO (Nigeria)." In Côte d'Ivoire, "Korea General Construction SL (KOGEN GE SL)" was registered in 2012. The website of the African Union Inter-African Bureau for Animal Resources lists KOGEN GE SL as its implementing partner for a project funded by Equatorial Guinea. KOGEN was separately reported as a contractor for the Rebola Municipal Stadium, completed in 2016, which documents suggest earned KOGEN approximately \$30.5 million. Local news claims that KOGEN opened a new, large national headquarters in Equatorial Guinea the same year⁴⁰.

Figure-4: I2 chart showing GENCO/KOGEN network



⁴⁰ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 56

GENCO Network

Source: *The Report of the UN Panel of experts pursuant UNSCR 1874, S/2019/171, p. 57.*

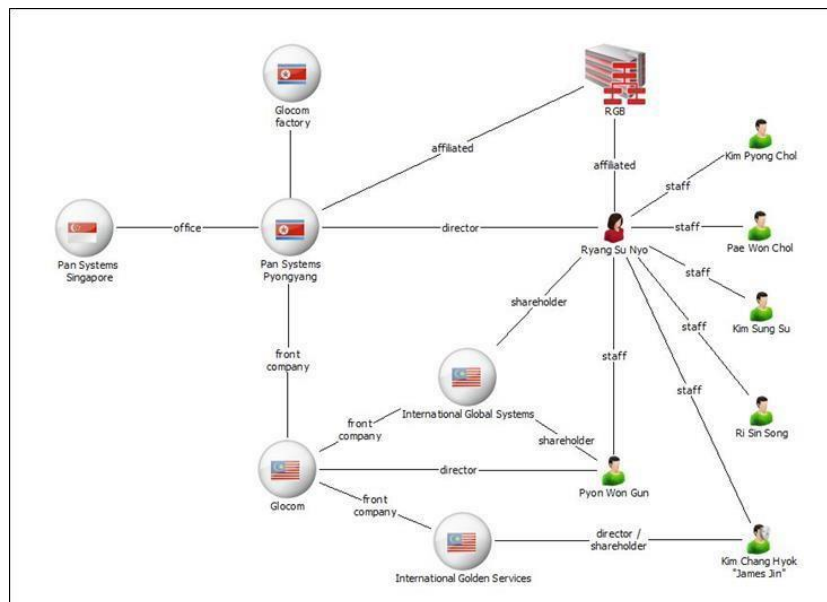
Analysis of GENCO/KOGEN bank accounts in Zambia, in dollars and in the local currency, showed regular cash and cheque activity and high account turnover. The accounts demonstrated similar patterns of cheque deposits, followed by incoming transfers, followed by regular cheque withdrawals⁴¹.

The Glocom Group

Glocom is a Malaysia based company that advertises radio communications equipment for military and paramilitary organizations. Glocom claims a presence in more than 10 countries and a prominent international reputation gained through participating, according to its website, in three biennial "Defense Service Asia" arms exhibitions since 2006. However, Glocom is not officially registered and has no presence at its listed physical address. Two other Malaysia based companies acting on its behalf: International Golden Services Sdn Bhd and International Global Systems Sdn Bhd⁴².

Figure-5: Pan Systems Pyongyang network

Source: Report of the UN Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 36.



Information obtained by the UN Panel of experts demonstrates that Glocom is a front company of the DPRK company Pan Systems Pyongyang Branch (Pan Systems

⁴¹ Report of the Panel of Experts pursuant UNSCR 1874, S/2019/171, p. 55

⁴² Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34

Pyongyang), which is linked to a Singaporean company named Pan Systems (S) Pte Ltd (Pan Systems Singapore)⁴³.

According to information obtained by the Panel, Pan Systems Pyongyang is operated by the Reconnaissance General Bureau, the country's premier intelligence agency, designated under UNSCR 2270 (2016). This shows how the Bureau enables its key agents to generate revenues for its operations through such networks. Additionally, the UN Panel of experts determined that "Wonbang Trading Co." is an alias of Pan Systems Pyongyang. The information shows that Pan Systems Pyongyang also regularly received funds from the Korea Mining Development Trading Corporation (KOMID)⁴⁴.

Financial Operations Of Glocom/Pan Systems Pyongyang

In its banking operations, Pan Systems Pyongyang and its front companies used an extensive network of individuals, companies, and offshore bank accounts to procure and market arms and related material. The global network consisted of individuals, companies, and bank accounts in China, Indonesia, Malaysia, Singapore, and the Middle East. In particular, €36,939 was transferred to International Global Systems in 2008 from an account at the Damascus branch of a Middle Eastern bank⁴⁵.

Since 1998, Pan Systems Pyongyang and International Global Systems have used accounts in United States dollars and euros at Daedong Credit Bank (a DPRK Bank) to gain access to the international financial system, including through bank accounts in China. These accounts were used to transfer funds to a supply chain of more than 20 companies located primarily on the Chinese mainland, in Hong Kong, China, and Singapore. In recent years, procurement shifted almost entirely to companies in China and Hong Kong, China. Most of these companies supplied electronic products, radio components, and casings consistent with Glocom's advertised military communications equipment, while others were transport companies. The network also made regular transfers to various facilitators with Chinese, Korean, foreign, and code names working in China, Indonesia, Malaysia, and the Middle East⁴⁶.

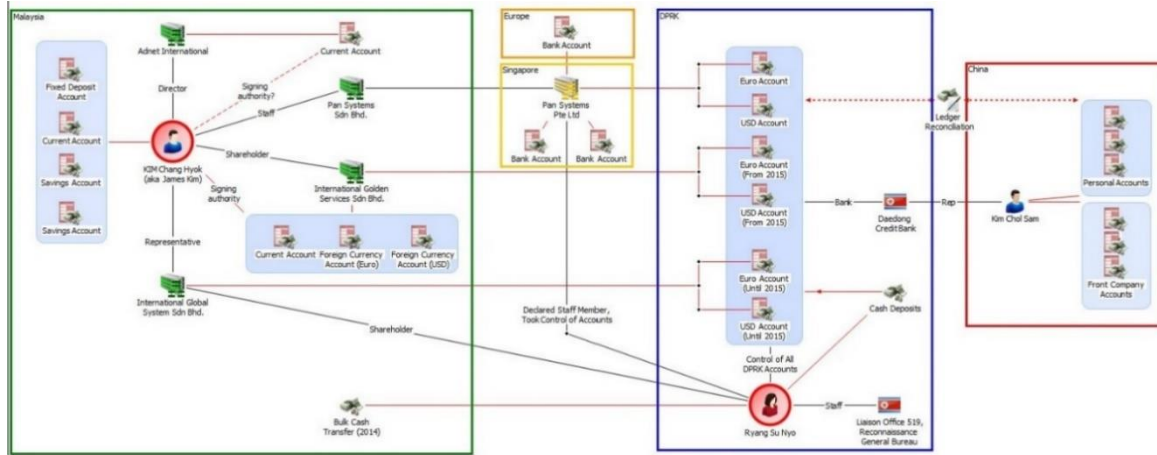
⁴³ Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 34

⁴⁴ Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 36

⁴⁵ Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77

⁴⁶ Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 77

Figure-6: Accounts controlled by Glocom



Source: Report of the UN Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 64

In terms of incoming transfers, Pan Systems Pyongyang received large remittances from an account at a major bank in Malaysia, as well as from numerous companies of the DPRK. Transfers were also made from the Shenyang consulate of the DPRK. Pan Systems Pyongyang also regularly used bulk cash transfers. In addition, Pan Systems Pyongyang received funds from two designated entities, KOMID and Hyoksin Trading Corporation. Between 2011 and 2013, Hyoksin made multiple euro-denominated transfers to Pan Systems Pyongyang, as did KOMID between 2011 and 2015⁴⁷.

In addition to its four bank accounts with the Daedong Credit Bank in Pyongyang, the Glocom network controlled at least 10 accounts in four other countries between 2012 and 2017, including through Malaysia-based front companies. Records show that these multiple overseas accounts allowed Glocom to continuously move funds between accounts it controlled in different banks and countries in the course of its illicit trade⁴⁸.

⁴⁷ Report of the Panel of Experts pursuant UNSCR 1874, S/2017/150, p. 78

⁴⁸ Report of the Panel of Experts pursuant UNSCR 1874, S/2018/171, p. 64

TFS - TF Red Flags

Considering the above typologies, the following are some red flags or indicators that could be looked at more closely or monitored by financial institutions and designated non-financial businesses or professions to identify TF potential sanctions circumventions of your clients, their business, or their transactions.

- 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 locations.
- 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 locations.
- 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 countries.
- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- 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 countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
- 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 ML/TF controls.
- Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- 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.
- Raising donations in an unofficial or unregistered manner.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g., crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of

- concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.
 - Client conducted travel-related purchases (e.g., purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
 - Individual or entity's online presence supports violent extremism or radicalization.
 - Irregularities during the CDD process which could include, but is not limited to:
 - Inaccurate information about the source of funds and/or the relationship with the counterparty.
 - Refusal to honor requests to provide additional KYC documentation or to provide clarity on the final beneficiary of the funds or goods.
 - Suspicion of forged identity documents
 - The following redflags are related to the use of Virtual Assets / Cryptocurrency:
 - The use of virtual assets to send funds to a few select wallets at unregulated virtual assets exchanges (or exchanges in territories where sanctioned people have influence or sanctioned jurisdictions).
 - Financial institutions should pay particular attention to the transfer of funds to a virtual assets exchange's operational banking account (to fund a virtual asset wallet) followed by the crypto-to-fiat conversion (either more or less) from the same exchange within a relatively short period of time.

TFS – PF Red Flags

Below are the Red-flags and Indicators of Possible Proliferation Financing to the 2018 FATF Typologies Report on Proliferation Financing that can help the public and private sector (FIs & DNFBPs) to detect any suspicious transactions to proliferation financing⁴⁹:

- Transaction involves person or entity in foreign country of proliferation concern.
- Transaction involves person or entity in foreign country of diversion concern.
- The customer or counterparty or its address is similar to one of the parties found on publicly available lists of “denied persons” or has a history of export control contraventions.
- Customer activity does not match business profile, or end-user information does not match end user’s business profile.
- A freight-forwarding firm is listed as the product’s final destination.
- Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- Transaction involves possible shell companies (e.g., companies do not have a high level of capitalisation or displays other shell company indicators).
- Transaction demonstrates links between representatives of companies exchanging goods i.e., same owners or management.
- Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g., does the country involved normally export/import good involved).
- Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
- Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
- New customer requests letter of credit transaction awaiting approval of new account.
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.

⁴⁹ FATF, 2018. *Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html

- Involvement of items controlled under WMD export control regimes or national control regimes.
- Involvement of a person connected with a country of proliferation concern (e.g., a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.
- Use of cash or precious metals (e.g., gold) in transactions for industrial items.
- Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
- Involvement of a customer or counterparty, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.
- Transactions between companies on the basis of “ledger” arrangements that obviate the need for international financial transactions.
- Customers or counterparties to transactions are linked (e.g., they share a common physical address, IP address or telephone number, or their activities may be coordinated).
- Involvement of a university in a country of proliferation concern.
- Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
- Evidence that documents or other representations (e.g., relating to shipping, customs, or payment) are fake or fraudulent.
- Use of personal account to purchase industrial items.
- The following Red-Flags are specific to proliferation Financing cases related to the UAE and other regional countries:
 - The use of representative offices of UNSC sanctioned banks to remit DPRK labours money to DPRK.
 - The use of extensive currency exchange networks to transfer bulk cash to Iranian nuclear program.
 - The use of cyber-attacks by the DPRK regime to steal funds from FIs and crypto currency exchanges.
 - Transactions involved in sale, shipment, or export of dual use goods on incompatible with technical level of the country being shipped (e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
 - Trade finance transaction involved shipment route with weak export control laws.
 - Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
 - The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.
 - Dealings with sanctioned goods or under embargo. For example:
 - Weapons
 - Oil or other commodities
 - Luxury goods (for DPRK sanctions)
 - Dealings with controlled substances / Dual-Use items.
 - Identifying documents that seemed to be forged or counterfeited.
 - Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
 - When the flows of funds exceed those of normal business (revenues or turnover).

- The activity developed or financed does not relate to the original or intended purpose of the company or entity. For example:
 - For companies, they are importing high-end technology devices, but they are registered as a company that commercializes nuts.
 - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide health services.
- Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.
- Carrying out of multiple ATM cash withdrawals in short succession (potentially below the daily cash reporting threshold) across various locations in territories where sanctioned people have influence or in the border of sanctioned countries.

References

ABC news, 2015. *US officials Ask HOW ISIS Got So Many Toyota Trucks*. [Online]
Available at: <https://abcnews.go.com/International/us-officials-isis-toyota-trucks/story?id=34266539>
[Accessed 13 April 2021].

AML Manual, 2021. *MONEY LAUNDERING AND TERRORIST FINANCING "RED FLAGS."* [Online]

Available at: <https://bsaaml.ffiec.gov/manual/Appendices/07>

[Accessed 5 October 2021].

Financial Action Task Force, February 2015. *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, Paris: FATF.

Financial Action Task Force, June 2014. *Risk of Terrorist Abuse in Non-Profit Organizations*, Paris: s.n.

Financial Action Task Force, October 2013. *The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing*, Paris: FATF.

Financial Action Task Force, October 2015. *Emerging Terrorist Financing Risks*, Paris: FATF.

FINTRAC, 2021. *Money laundering and terrorist financing indicators—Financial entities*. [Online]

Available at: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/fin_mltf-eng

[Accessed 5 October 2021].

FATF, 2018. *Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, Paris, FATF. [Online]

Available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html

[Accessed 5 October 2021].

NCBC News, 2020. *NCBCNews.com*. [Online]

Available at: <https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329>

[Accessed 21 September 2020].

Panel of Experts pursuant to UNSCR 1874, S/2020/151. *Report of the Panel of Experts established pursuant to UNSCR 1874*, New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2017/150. *Report of the Panel of Experts established pursuant to resolution 1874*, New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2018/171. *Report of the Panel of Experts pursuant UNSCR 1874*, New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/171. *Panel of Experts Report Pursuant UNSCR 1874 S/2019/171*, New York: United Nations Security Council.

Panel of Experts pursuant UNSCR 1874, S/2019/691. *Report of the Panel of Experts established pursuant to resolution 1874 (2009)*, New York: United Nations Security Council.

U.S. Department of the Treasury, 2016. *Press Center*. [Online]
Available at: <https://www.treasury.gov/press-center/press-releases/pages/jl0322.aspx>
[Accessed 1 February 2021].

U.S. Department of Treasury , 2018. *Press Releases*. [Online]
Available at: [https://home.treasury.gov/news/press-releases/sm0383#:~:text=Washington%20%E2%80%93%20Today%20the%20United%20States,IRGC%2DQF\)%20to%20fund%20its](https://home.treasury.gov/news/press-releases/sm0383#:~:text=Washington%20%E2%80%93%20Today%20the%20United%20States,IRGC%2DQF)%20to%20fund%20its)
[Accessed 1 January 2021].

United Nations Counter-Terrorism Committee Executive Directorate and the Analytical Support and Sanctions Monitoring Team pursuant to resolutions 1526 (2004) and 2253 (2015), S/2020/493. *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)*, New York: United Nations Security Council.

United Nations Office on Drugs and Crime, 2012. *The Use of the Internet for Terrorist Purposes*, New York: UNODC.

United Nations Security Council, 2014. *Resolution 2178* , s.l.: s.n.

www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware, 2018. *FASTCash: How the Lazarus Group is emptying millions from ATMs..* [Online]
Available at: www.symantec.com/blogs/threat-intelligence/fastcash-lazarus-atm-malware.

Emerging Terrorist Financing Risks October 2015

Available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>

Ethnically Or Racially Motivated Terrorism Financing June 2021

Available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/Ethnically-or-racially-motivated-terrorism-financing.pdf>

Document Change Log

The following main amendments have been made to the Typologies on Circumvention of the Targeted Sanctions Against Terrorism and Proliferation of Weapons and Mass Destruction since the text was adopted in March 2021.

Page Number	Type of amendments	Sections subject to amendments
8	Addition of a new section and case study	To add a section to clarify the trends and methods that can be used to Finance the “Houthies Movement” by including a case study.
12 & 13	Addition of two case studies	To add two case studies to “NPO Affiliation with Terrorist Entity” section.
15	Addition of a case study	To add a case study that demonstrate the trade of dual use by a terrorist group (Somalia Youth Movement).
17 & 18	Addition of two case studies	To add two case studies to the section titled “Misuse of legal entities” to elaborate more about the methods used in Sanction Evasion.
18 & 19	Addition of new section	To add a new section on using virtual assets to support TFS
-	Deletion of section	To delete the section under the title “Indirect Making economic resources available”.
26	Addition of a case study	To add a case study under the title of the section “Smuggling Petrochemicals”.
28	Addition a case study	To add a case study to demonstrate the international cooperation for countering Proliferation Financing.

35 - 39	Rearrange the TFS-Red flags	To rearrange the red flags to include to separated sections one for “TFS- TF Red Flags” and the other for “TFS-PF Red Flags”.
---------	-----------------------------	---

Targeted Financial Sanctions Instructions for the Private Sector on Sanctions Lists Updates

Upon receipt of an update related to either the UAE Local Terrorist List or the United Nations Consolidated List, you must complete the following actions:

1. **Screen** whether you have or have had a relationship with the designated individuals or entities.
2. **Freeze immediately, and in any case within 24 hours** (*from the designation being made*), the funds or other assets⁽¹⁾ owned or controlled, directly or indirectly, by the designated individuals or entities.
3. **Refrain** from providing funds or other assets or services, directly or indirectly, to the designated individuals or entities unless granted permission by the Executive Office.
4. **Report** ⁽²⁾ to the Executive Office and your respective Supervisory Authority via the goAML platform ⁽³⁾:
 - For a 'Confirmed Match', submit a **Fund Freeze Report (FFR)** within five business days along with all the necessary information and documents.
 - For a 'Potential Match', submit a **Partial Name Match Report (PNMR)** within five business days along with all the necessary information and documents.

Note: An STR/SAR should not be used to report confirmed or potential name matches for persons designated on the UAE Local Terrorist List or the UN Consolidated List.

For any inquiries regarding sanctioned individuals or entities, please contact us by email: iec@uaeiec.gov.ae

Note-1: Definition and examples of "funds or other assets" as per the published TFS Guidance – Section 3

Note-2: For more information on reporting obligations, refer to the published TFS Guidance – Section 4

Note-3: If you are not a goAML user, report by sending an email to iec@uaeiec.gov.ae.