

TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM, TERRORISM FINANCING AND PROLIFERATION TRAINING POLICY



This Manual is the sole property of RV INTERNATIONAL FZCO and is meant exclusively for its internal use. It is strictly forbidden to make or reproduce a copy of this Manual in any form, in part or in whole, without the prior written consent of the Owner/ Senior Management.

VERSION: /V.2

DOCUMENT CONTROL

TITLE	Targeted Financial Sanctions Related to Terrorism, Terrorism Financing and Proliferation Training Policy
Information Classification	INTERNAL
Policy Supported	RV INTERNATIONAL FZCO
Current Version	V.2
Review Cycle	ANNUALLY
Effective Date	May 2026
Due Date for Review	April 2027

Document Contact details

ROLE	DESIGNATION
REVIEWED BY	SENIOR MANAGEMENT
APPROVED	OWNER

Document Revision History:

Rev No	Effective Date	Revision History	Due Date
V.1	January 2025	Initial Creation	December 2025
V.2	May 2026	FEDERAL LAW 10 OF 2025 AMENDMENT FOCUSING ON TAX EVASION, PREDICATE CRIME AND PENALTY FOR ENTITIES UPTO AED 100,000 MILLION AS PER ARTICLE 27 CABINET RESOLUTION NO. (134) OF 2025 REGARDING THE EXECUTIVE REGULATIONS OF FEDERAL DECREE BY LAW NO. (10) OF 2025 REGARDING ANTI-MONEY LAUNDERING, AND COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION FINANCING.	April 2027

Policy Approval

The undersigned acknowledge that they have been reviewed by Senior Management. Any further changes to this Policy in future can only be recommended by Senior Management and approved by the Owner.

TABLE OF CONTENTS

1	INTRODUCTION.....	7
2	GUIDELINE ON GRIEVANCE PROCEDURES.....	7
3	PURPOSE OF THIS POLICY	8
4	DEFINITION OF “FUNDS”	8
5	JURISDICTION’S SANCTIONS REGIME.....	8
6	LEGAL BASIS/SANCTIONS AUTHORITIES.....	9
6.1	TYPES OF FINANCIAL SANCTIONS	11
6.2	HOW TO IDENTIFY A MATCH TO APPLY TFS?	12
6.3	PREDICATE OFFENSES	13
6.4	THE FINANCING OF TERRORISM.....	14
6.5	FINANCING OF ILLEGAL ORGANISATIONS	14
6.6	TRADE BASE MONEY LAUNDERING	14
6.7	ATTEMPTED TRANSACTION.....	16
6.8	REPORTING ENTITY.....	16
7	OBJECTIVES OF FINANCIAL SANCTIONS	16
8	POLICY COMPLIANCE AND CUSTODIAN	16
9	COMPLIANCE AND ENFORCEMENT OF THIS POLICY.....	16
10	DEFINITION - TARGETED FINANCIAL SANCTIONS.....	17
11	WHAT IS UNITED NATIONS SECURITY COUNCIL RESOLUTION (UNSCR)?	17
12	THE FATF’S COMMITMENT TO TFS.....	17
13	FEATURES OF FATF RECOMMENDATION 6 – TFS RELATED TO TERRORISM AND TERRORIST FINANCING (SOURCE: FATF METHODOLOGY 2013)	17
14	WHAT IS PROLIFERATION FINANCING OF WEAPONS OF MASS DESTRUCTION (PF-WMD)? 18	
15	UN SECURITY COUNCIL’S APPROACH TO COUNTER TF AND PF-WMD.....	18
16	UNSCRS WHICH ARE RELEVANT TO YOU AS FIS	18
17	LEGISLATION ON FINANCIAL	18
18	THE OBLIGATION TO FREEZE ‘WITHOUT DELAY’ DEFINED	18
19	PROTECTION AGAINST LIABILITY FOR REPORTING PERSONS	19
20	THE FINANCING OF TERRORISM	19
21	SANCTIONS	19
21.1	WHAT IS A SANCTIONS LIST?	19
21.2	HOW DOES SANCTIONS SCREENING WORK?	22
21.3	WHEN SHOULD SANCTIONS SCREENING BE PERFORMED TO ENSURE SANCTIONS COMPLIANCE?.....	22

21.4	SANCTIONS SCREENING CHALLENGES.....	23
21.5	CUSTOMER SCREENING	25
21.6	NAME SCREENING	25
21.7	VERIFICATION OF FALSE POSITIVES	26
21.8	PAYMENTS SCREENING	27
21.9	CONFIRMED MATCH.....	27
21.10	NOTIFICATION TO EXECUTIVE OFFICE	27
22	RED FLAG INDICATORS/SUSPICIOUS INDICATORS	28
23	SANCTIONS COMPLIANCE PROGRAM.....	31
24	EO IEC'S ROLE	32
25	SENIOR MANAGEMENT COMMITMENT	32
26	RISK ASSESSMENT	32
27	SANCTIONS RISK APPETITE	34
28	INTERNAL CONTROLS	34
29	POLICIES AND PROCEDURES	34
30	TRAINING	35
31	INDEPENDENT AUDIT AND TESTING OF PROCESSES AND SYSTEMS.....	35
32	RECORD KEEPING.....	36
33	OVERVIEW OF TARGETED FINANCIAL SANCTIONS	36
	SECTION 1: LEGAL FRAMEWORK.....	36
	SECTION 2: TARGETED FINANCIAL SANCTIONS DEFINITION AND SCOPE.....	37
	SECTION 3: THE PURPOSE OF TFS	39
	SECTION 4: TFS OBLIGATIONS	41
	SECTION 5: OWNERSHIP, CONTROL, AND ACTING ON BEHALF OR AT THE DIRECTION OF DESIGNATED PERSONS.	47
	SECTION 6: ENFORCEMENT MEASURES	47
	SECTION 7: OBLIGATIONS REGARDING UNILATERAL / MULTILATERAL SANCTIONS REGIMES AND SANCTIONS EVASION	48
	ANNEXURE I: EOCN NOTIFICATION ALERT SYSTEM SUBSCRIPTION GUIDE.....	49
	ANNEXURE II TFS REPORTING FLOW CHARTS	53
	ANNEXURE III FREQUENTLY ASKED QUESTIONS.....	53

COMPANY PROFILE

Legal Name as per Trade License : RV INTERNATIONAL FZCO

Legal Type : Free Zone Company

DNFBP Category : Dealers in Precious Metals and Stones

Licensing Authority : DMCC

License Number : DMCC-174001

Incorporation Date : 9-Mar-2016

Principal Activities : Basic Non Ferrous Metal Products Trading, Non- Manufactured
Precious Metal Trading, Grains, Cereals & Legumes Trading,
Ships & Boats Trading

Authorized Person Name : Raghav Bansal

MLRO/ Compliance Officer : Rahul Bansal

Office Address : Office 47J, Almas Tower, Jumeirah lake towers, Dubai, UAE

Mobile Number : 052-8628634/055-9841203

Phone Number : 052-8628634/055-9841203

Email id : rahul.bansal@rvinternationaldmcc.com

DETAILS OF BENEFICIAL OWNER

S. N	NAME	NATIONALITY	ID NUMBER	SHAREHOLDING %
1	Raghav Bansal	Indian	784-1992-7310496-0	100%

TERMINOLOGY AND DEFINITIONS

TERMS	DESCRIPTION
Freezing	To prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by individuals, entities, or groups designated on the UAE Local Terrorist List or United Nations Consolidated List
Local Terrorist List	National terrorist list issued by the UAE Cabinet
Person	All natural and legal persons
Reporting Entities	These comprise FIs, DNFBPs, and VASPs that are obligated to comply with the AML/CTF/CPF laws of the UAE
Sanctions Committee	United Nations Security Council Sanctions Committee that oversees compliance of United Nations Security Council Resolutions. Please note that all current United Nations sanctions regimes have their own Sanctions Committee
Sanctions Lists	UAE Local Terrorist List and UNSC Consolidated List
Supervisory Authority	Federal and local authorities which are entrusted by legislation to supervise FIs, DNFBPs, VASPs or the authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislation
UNSC Consolidated List	United Nations Security Council Consolidated List pursuant to the relevant United Nations Security Council Resolutions
Without Delay	Immediately or in any case within 24 hours upon designation of an individual, entity, or group on the UAE Local Terrorist List or UNSC Consolidated List.

1 INTRODUCTION

In today's global financial environment, compliance with Targeted Financial Sanctions (TFS) is a critical responsibility for Financial Institutions (FIs), Designated Non-Financial Businesses and Professions (DNFBPs), and Virtual Asset Service Providers (VASPs)—collectively referred to as “Reporting Entities” operating in the United Arab Emirates (UAE) and globally. TFS are designed to prevent the abuse of financial systems for illicit purposes, such as terrorism financing (TF), proliferation financing (PF), and sanctions evasion. Following are the scenarios where target financial sanctions are required to be monitored:

- Asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.
- Designated persons and entities – Lists of “bad actors” who threaten the world peace (terrorism / proliferation)
- The lists are updated by the Security Council regularly.
- UN member countries can't do financial dealings with such designated individuals and entities.

Given the significant role of the private sector in the UAE, it is essential that RV INTERNATIONAL FZCO implement TFS effectively, maintain strong compliance frameworks, and meet the country's legal requirements. This guideline aims to clarify the obligations of RV INTERNATIONAL FZCO under the UAE's TFS legal regime and outlines the scope and definition of applicable sanctions measures.

Key obligations include:

1. **Registration** with the Executive Office of Anti-Money Laundering and Counter Terrorism Financing (EOCN)'s Notification Alert System (NAS).
2. **Screening** against the UAE's Local Terrorist List and the United Nations Security Council Consolidated List.
3. **Freezing assets** of designated persons without delay and prohibiting the availability of funds or assets to such individuals or entities.
4. **Reporting** actions taken under TFS obligations.

Additionally, the guideline explains important concepts such as ownership and control as they relate to TFS, and outlines potential enforcement actions in cases of non-compliance. It also provides guidance on obligations related to the implementation of both unilateral and multilateral sanctions.

This document is an update to the previous version of the UAE's TFS Guidance (revised in September 2022). Key updates include:

- Renaming the “Funds Freeze Report (FFR)” to the “Confirmed Name Match Report (CNMR)” for reporting confirmed matches.
- Added clarifications and examples for reporting **Partial Name Matches**.
- New guidance on conducting screenings and implementing freezing measures during weekends and public holidays.
- Procedures for submitting grievance requests have been removed and are now covered in a separate

2 GUIDELINE ON GRIEVANCE PROCEDURES.

We recognize the importance of having formal, documented TFS policies and procedures. Our commitment to regulatory compliance reflects our dedication to ethical business practices and risk management. By implementing and adhering to these measures, we ensure that our business remains compliant with sanctions regulations and avoids inadvertent dealings with designated individuals or entities.

As a retail and wholesale distribution network involved in cross-border transactions, it is crucial to conduct enhanced due diligence on suppliers, partners, and clients. TFS policies provide an added layer of protection and reinforce trust and transparency in our business operations.

Our proactive approach underscores our understanding of the importance of sanctions compliance and the potential risks of non-compliance. By remaining vigilant, we protect our company's reputation and maintain high standards of service for our clients.

3 PURPOSE OF THIS POLICY

This policy is intended to support our sector in building robust systems for sanctions compliance and to promote our active participation in the fight against terrorism financing, proliferation financing, and other TFS-related threats. It also aims to help our organization fulfill its training and implementation obligations under TFS regulations.

4 DEFINITION OF "FUNDS"

"any assets, economic resources, property of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, wherever located, legal documents or instruments in any form, electronic or digital, evidencing title to, or interest in, such assets, economic resources or property, including but not limited to currency, bank credits, deposits and other financial resources, travelers cheques, bank cheques, money orders, promissory notes, shares, non-shareholding interest, securities, bonds, drafts, letters of credit, and any interest in, dividends or others income on or value accruing from or generated by, in full or in part, any such assets, economic resources or property."

5 JURISDICTION'S SANCTIONS REGIME

The United Arab Emirates ("UAE") has a complex sanctions regime based on a variety of sources. Sanctions are based on diverse interests, including political, economic, and national security interests. Due to the rapidly changing nature of such interests, sanctions are susceptible to significant and constant changes.

Sanctions in the UAE are usually imposed at a federal level, through a variety of methods, including, by way of example:

Adding sanctioned persons to local lists and the United Nations ("UN") sanctions list: This is effected by issuing local terrorism lists ("Local Lists") and implementing the sanctions passed by the UN Sanctions Committee ("Sanctions List") pursuant to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in the UAE is Federal Decree No. (20) Of 2018 On Anti-Money Laundering And Countering The Financing Of Terrorism ("Federal Decree"). This Law Has Been Repealed By The Federal Decree By Law No. (10) Of 2025 Regarding Anti-Money Laundering, And Combating The Financing Of Terrorism And Proliferation Financing. (the "AML-CFT Law" or "the Law") Cabinet Decision No.10 2019 concerning the Implementing Regulation of the AMLCFT Law ("New Sanctions Regulations") which is repealed by Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing, the recent Cabinet Decision No 74 of 2020 concerning the UAE List of Terrorists and the 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 ("New Sanctions Regulations") and Federal Law No. 7 of 2014 on Combatting Terrorism Offences. Guidance was issued on targeted financial sanctions by the Executive Office of the Committee for Goods and Materials subject to Import and Export Control ("Office") on 6 May 2021 further setting out the implementation of the New Sanctions Regulations (the "New SR Guidance").

UAE and international sanctions such as those of the UN, Office of Foreign Assets Control ("OFAC") and the European Union ("EU"), as applicable. As a member of the UN, the UAE is required to comply with all sanctions passed by the UN Security Council.

There have been significant changes or developments impacting the UAE sanctions regime over the past 12 months.

Notably, from a legislative framework perspective, the UAE's previous sanctions regulations and implementation regulations were abrogated, and new such legislation was issued. From a substantial perspective, among other

changes, compliance obligations and required steps by UAE persons have increased, as illustrated in the New SR Guidance.

6 LEGAL BASIS/SANCTIONS AUTHORITIES

The legal or administrative authorities for imposing sanctions. The Supreme Council for National Security, the UAE Cabinet and the UN Security Council are the ultimate entities responsible for imposing sanctions. The Supreme Council for National Security proposes sanctions both internally and to the UN Sanctions Committee pursuant to Article 2 of the New Sanctions Regulations.

JURISDICTION IMPLEMENTS UNITED NATIONS SANCTIONS

The process of significant ways in which company implemented United Nations sanctions.

DNFBPs and FIs are subject to additional obligations as set out in the New SR Guidance. These include setting internal controls and procedures to ensure compliance with the New Sanctions Regulations, as well as policies and procedures to prohibit staff from informing any customer or third party of impending freezing action.

It is worth noting that in certain cases, sanctions imposed by the UN may have already been implemented by the UAE on other grounds and included in Local Lists, e.g., as a result of its membership in the Terrorist Financing Targeting Centre (“TFTC”).

The UAE is a member of three main regional bodies that issue sanctions – the Arab League, the TFTC and the Gulf Cooperation Council (“GCC”).

- ✚ **Arab League:** The UAE implements sanctions adopted by the Arab League on an ad hoc basis.
- ✚ **TFTC:** Members of the TFTC consist of the United States and certain GCC countries.
- ✚ The UAE implements all sanctions designated by the TFTC by issuing the Local Lists referred to above. TFTC designated sanctions are also available on the US’s treasury government website.
- ✚ **GCC:** The UAE is a member of the GCC, which consists of six member states. The Charter of the GCC sets up a framework that would permit the joint establishment of foreign policies and therefore issuance of sanctions. Although the GCC has, in the past, made announcements with respect to its members’ stance on foreign policy. It has not, at the date hereof, issued any sanctions as such.

JURISDICTIONS MAINTAIN ANY LISTS OF SANCTIONED INDIVIDUALS AND ENTITIES.

Were the individuals and entities: a) added to those sanctions lists and b) removed from those sanctions lists.

The UAE maintains two lists of sanctions individuals and entities:

- ✚ **Local Lists:** These lists consist of local terrorism lists issued pursuant to Federal Law No. 7 of 2014 on combatting terrorism offences (“Anti-Terrorism Law”) and the New Sanctions Regulations. Decisions of listing, removal and re-listing on Local Lists enter into effect when issued by the UAE Cabinet and when published in the Official Gazette. Such decisions are also published in audio-visual and print media of the UAE, in both Arabic and English.
- ✚ **Sanctions List:** This list consists of the sanctions list issued by the UN Security Council. Additions and/or removal from the sanctions list are effected by the UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.

A. Can the public access those lists?

Both the consolidated Local List and Sanctions List are available via the following links:

- I. With respect to the Local List (<https://www.uaieec.gov.ae/en-us/un-page>)
- II. With respect to the Sanctions List (<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>)

There is also a direct link to the UN sanctions on the official website.

B. Comprehensive sanctions or embargoes against countries or regions

The UAE used to maintain comprehensive sanctions or embargoes on Qatar and Israel, however, these were recently removed and there are no current comprehensive sanctions or embargoes on countries as such. By implementing the UN's sanctions, the UAE does have targeted sanctions against Central African Republic, Congo, Iraq, Libya, Mali, Somalia, South Sudan and Yemen.

C. JURISDICTION MAINTAINS ANY OTHER SANCTIONS.

In addition, to the above-mentioned sanctions, the UAE, the regulated FIs in the UAE, also takes into consideration sanctions imposed by the EU and OFAC; however, where implemented, such sanctions would be added to its lists accordingly.

D. IMPLEMENTATION OF SANCTIONS LAWS AND REGULATIONS

- Parties and transactions are subject to your jurisdiction's sanctions laws and regulations. For example, do sanctions restrictions apply based on the nationality of the parties involved or the location where the transactions take place?
- The parties and transactions subject to UAE's sanctions laws and regulations depend on the nature of and reasons for the sanctions.
- Certain sanctions are more narrowly targeted than others. With respect to sanctions targeted at specific individuals and organizations (e.g. under Local Lists), restrictions would not apply based on nationality but rather on identity or affiliations. With respect to more comprehensive sanctions targeted at governments, such sanctions can apply based in the nationality of persons involved.
- Sanctions can also apply on the location where the transaction takes places, this is particularly relevant where sanctions are targeting trade with a certain country or the country imposing the sanction refuses to recognize or accept deals involving the currency of a certain country, as is the case with Iran.

E. ARE PARTIES REQUIRED TO BLOCK OR FREEZE FUNDS OR OTHER PROPERTY THAT VIOLATE SANCTIONS PROHIBITIONS?

Under Article 15 of the New Sanctions Regulations and under the New SR Guidance, there is an express obligation on FIs, DNFBPs, and all natural and legal persons to block or freeze funds or other property belonging to persons on the sanctions list ("Designated Persons").

- If a match is identified with a Designated Person, they must freeze all funds owned by such person, prohibit the making of funds available, and notify the Office of such measures within two business days of taking such measures.
- In addition to the above, FIs and DNFBPs must set and implement internal controls and procedures as well as policies and procedures to ensure their and their staff's compliance with the New Sanctions Regulations and that no one tips off any Designated Person of impending measures.

F. ARE THERE LICENSES AVAILABLE THAT WOULD AUTHORIZE ACTIVITIES OTHERWISE PROHIBITED BY SANCTIONS?

There are no licenses available that would authorize activities otherwise prohibited by sanctions per se. However, special licenses may be required to conduct activities more susceptible to the possible breach of sanctions; for example, pursuant to the Commodities Law, strategic goods and dual –use items, such as arms and military hardware, chemical and biological materials cannot be exported or re-exported without a special license.

G. ARE THERE ANY SANCTIONS RELATED REPORTING REQUIREMENTS? WHEN MUST REPORTS BE FILED AND WHAT INFORMATION MUST BE REPORTED?

Multiple laws and regulations, including Article 15 of the AMLCFT Law, impose an obligation on FIs and DFNBPs to report to the relevant financial regulator any suspicion or any situation in which they have reasonable grounds to suspect a transaction or funds is related to a money laundering crime, related predicate offences, financing of terrorism or illegal organizations.

H. THE GOVERNMENT CONVEYS ITS COMPLIANCE EXPECTATIONS

Are certain entities required to maintain compliance programs? What are the elements of a compliance program required (or recommended) by the competent regulator(s)?

The government conveys its compliance expectations by circulating circulars and directives as well as issuing laws, regulations and guidance, in particular its New SR Guidance.

Article 16 of the AMLCFT Law, as well as the New SR Guidance, require FIs and DFNBPs to develop internal policies, controls, and procedures to enable them to manage the risks identified and mitigate them.

6.1 TYPES OF FINANCIAL SANCTIONS

Financial sanctions are measures imposed by governments or international organizations to influence or deter specific behaviors by individuals, organizations, or countries. These sanctions typically aim to address issues such as money laundering, terrorism financing, human rights violations, or violations of international law. The main types of financial sanctions include:

1. Asset Freezes (or Asset Blocking)

These sanctions freeze the assets and financial resources of individuals, entities, or governments, preventing them from accessing or using their funds or property in the jurisdiction enforcing the sanctions. Asset freezes are often imposed on persons or organizations associated with terrorism, money laundering, or other illicit activities.

2. Trade Restrictions

These sanctions restrict or prohibit specific financial transactions or trade activities. They can target goods, services, or sectors of the economy that are considered to be contributing to illegal activities, such as arms trafficking, or the financing of terrorism. Trade sanctions may include bans on exports, imports, or financial services to certain individuals or countries.

3. Blocking of Financial Transactions

This type of sanction restricts or completely blocks the ability of a designated entity or individual to conduct financial transactions. This includes prohibiting access to international financial markets or banking systems, thus cutting off the target from international economic systems.

4. Prohibition of Business or Financial Relationships

These sanctions prohibit domestic businesses or financial institutions from engaging in business or financial relationships with specific foreign individuals, entities, or governments. This is often intended to limit the target's ability to access funding or services from international financial institutions or markets.

5. Targeted Sanctions (Smart Sanctions)

These are narrowly focused measures aimed at specific individuals, entities, or sectors rather than broad, country-wide sanctions. Targeted sanctions may include asset freezes, travel bans, or restrictions on doing business with certain persons or entities involved in human rights abuses, terrorism, or other unlawful activities.

6. Export Control Sanctions

These sanctions regulate or restrict the export of sensitive technologies, goods, or services that could contribute to the development of weapons of mass destruction, military capabilities, or other dangerous activities. Export control sanctions may apply to specific industries, such as aerospace or nuclear technology.

7. Debt and Equity Restrictions

These sanctions prohibit the provision of loans, credit, or investments to sanctioned entities or individuals. They may also prevent individuals or companies from purchasing or trading debt and equity securities issued by the targeted entity, limiting their ability to raise capital.

8. Secondary Sanctions

Secondary sanctions are imposed on foreign entities or individuals that continue to do business with those already under primary sanctions. This extends the reach of sanctions beyond the initial target to deter other parties from engaging in prohibited activities with the sanctioned individuals or governments.

9. Comprehensive Sanctions

These are broad, country-wide measures that block nearly all financial, trade, and economic interactions with a particular country. These sanctions are typically reserved for situations involving serious international law violations, such as acts of aggression or violations of human rights.

Each type of financial sanction serves a different purpose, from isolating specific actors from the global financial system to promoting compliance with international laws and norms. Financial sanctions can have significant economic impacts on the targeted individuals or countries, while also influencing broader geopolitical dynamics.

The target financial sanctions are implemented in the UAE following UNSCR with relation to:

- Terrorism and terrorist financing
- The proliferation of weapons of mass destruction (WMD)
- Other UN sanctions regimes with TFS

6.2 HOW TO IDENTIFY A MATCH TO APPLY TFS?

To identify must screen on a going basis, and at least daily, their customers, potential customers, beneficial owners, and transactions to identify possible matches to the Local Terrorist List or UN List. Sanctions Lists contain a range

of information to aid the identification of listed individual or entity. The following are examples of the information contained in the Sanctions lists:

For Natural Person	For legal person
• Name • Aliases • Date of birth • Nationality • ID or Passport information • Last known address	• Name (s) • Aliases • Address of registration • Address of branches • Other information

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

When identifying the potential match, suspend any transaction until you can be satisfied it is not an individual or entity subject to TFS. (“False positive result”).

Note that: If the individual or entity you are dealing with matches all or most of the information on any of the Sanctions Lists, then this is likely to be a confirmed match. In this case, you must implement the freezing measures immediately, refrain from offering any funds or services, and notify the relevant Supervisory Authority and the Executive Office immediately.

- **Potential Match:** A potential match is when there is any match between data in the Sanctions Lists with any information in your databases.
- **Confirmed Match:** A confirmed match is when a potential match has been confirmed to be the individual, group or entity subject to TFS or when there is any doubt, indication, or suspicious that the potential match may correspond to individual, group or entity subject to TFS.
- **False Positive Result:** False positive result is when a potential match was discharged.

6.3 PREDICATE OFFENSES

The AML-CFT Law defines a predicate offence as “any act constituting an offence or misdemeanor under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.” A predicate offence is therefore any crime, whether felony or misdemeanor, which is punishable in the UAE, regardless of whether it is committed within the State or in any other country in which it is also a criminal offence.

FATF has designated 21 (twenty-one) major categories comprising many individual predicate offences. Each of these categories of predicate offences has been criminalized in the legislative framework of the State. Supervised institutions are reminded that this is not an exhaustive list of predicate offences, but simply a convenient categorization, since in the UAE according to the AML-CFT Law, even crimes that do not appear on this list, whether felonies or misdemeanors, can be predicate offences to money laundering.

Based on expert analysis of these categories conducted on behalf of the UAE’s Competent Authorities for the 2018 National Risk Assessment, the top (highest) threats to the State in relation to money laundering have been identified

as: fraud, counterfeiting and piracy of products, illicit trafficking in narcotic drugs and psychotropic substances, and professional third-party money laundering

6.4 THE FINANCING OF TERRORISM

Financing of Terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity. Funds may involve low dollar value transactions and give the appearance of innocence and a variety of sources. Funds may come from personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organize fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but all the funds are actually transferred to a terrorist group. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism you may have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place are Supervised. However, like money launderers, terrorism financiers also move funds to disguise their source, destination and purpose for which the funds are to be used. The reason is to prevent leaving a trail of incriminating evidence - to distance the funds from the crime or the source, and to obscure the intended destination and purpose.

Offering, collecting, ensuring access to, or transporting funds by any direct or indirect means to any society, organization, establishment, center, group, gang or any other persons to whom the provisions of Federal Law No. (7) Of 2014 regarding terrorist acts, apply. The UAE, cognizant of the need for regulatory legislation, has enacted numerous laws at federal level to prevent and criminalize money laundering and the financing of terrorism.

6.5 FINANCING OF ILLEGAL ORGANISATIONS

The AML-CFT Law treats the financing of illegal organizations as a criminal offense with no statute of limitations. It criminalizes actions such as money laundering where the individual knows the proceeds are linked to an illegal organization, even if there is no intent to conceal the illicit origin. Additionally, it includes actions where someone knowingly provides or facilitates the collection of funds intended to benefit an illegal organization or its members.

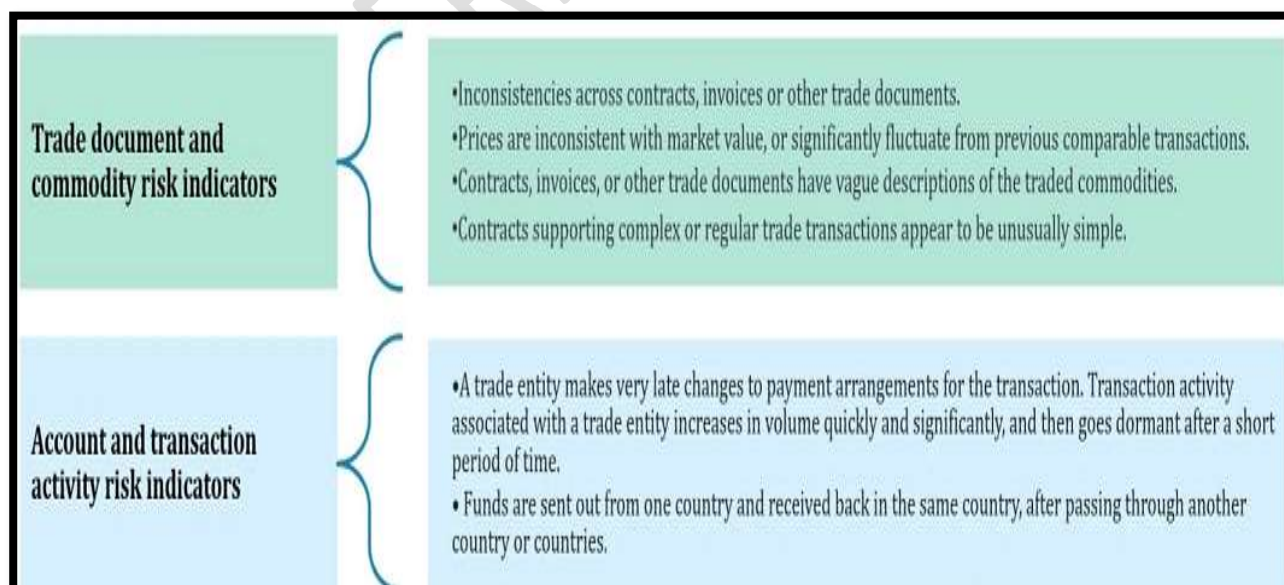
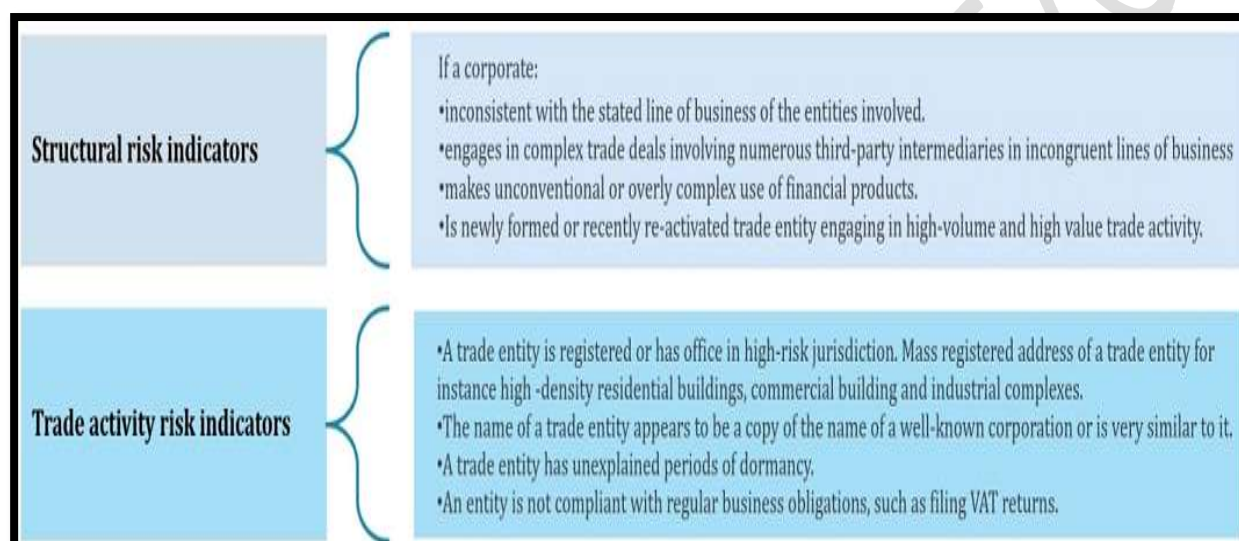
When assessing risks related to the financing of illegal organizations, Designated Non-Financial Business and Professions (DNFBPs) are advised to focus on the regulatory and financial transparency of organizations they engage with, especially non-profits, social, religious, or cultural groups. This is crucial when dealing with organizations in jurisdictions with limited transparency or access to information.

6.6 TRADE BASE MONEY LAUNDERING

The value of precious metals and stones varies highly based on their quality and purity, features which may not be apparent to the naked eye. In addition, the value of certain precious stones, particularly diamonds, can differ for different non-industry customers based on their personal preferences. This makes precious metals and stones particularly vulnerable to TBML, in which illicit actors use supposedly or actually licit trade to hide illicit finance.

- Trading the same goods—often precious stones—repeatedly between co-conspirators to justify funds transfers between members of a criminal network, or between companies owned by the same individual(s). In these schemes, a single precious stone may be repeatedly sold between members of the network, or a single stone may be sold to multiple “purchasers” at the same time, each time with a different description.

- Inflation or deflation of the value of traded stones to provide justification for cross-border transfers. A merchant may sell low-value precious metals or stones to a purchaser, but invoice for higher-quality goods and thus a higher sum. The purchaser pays the full invoice price, justifying the transaction to financial institutions, and also receives illicit goods such as drugs or smuggled items.
- Use of precious metals and stones as security for fraudulent loans. In a typology that is often related to TBML, precious metals or stones may be repeatedly sold or falsely valued between members of a network in order to justify loans and other forms of financing.
 - Trading gold to legitimize the proceeds of drugs trafficking.
 - Large –Scale sanctions evasion using precious metals.
 - Over valuation



6.7 ATTEMPTED TRANSACTION

Is one where a customer intended to conduct a transaction and took some form of action to do so it is different from a simple request for information, such as an enquiry as to the price of a certain item? An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the customer.

6.8 REPORTING ENTITY

If a DNFBP suspects, or has reasonable grounds to suspect, that any transaction, proposed transaction or attempted transaction is related to ML/TF or other serious crime, our company required to immediately file a Suspicious Transaction Report (STR) to the FIU.

7 OBJECTIVES OF FINANCIAL SANCTIONS

Financial Sanctions are imposed to:

1. Coerce a regime, or individuals within a regime, into changing their behavior (or aspects of it) by increasing the cost on them to such an extent that they decide to cease the offending behavior,
2. Constrain a target by denying them access to key resources needed to continue their offending behavior, including the financing of terrorism or nuclear proliferation.
3. Signal disapproval, stigmatizing and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or
4. Protect the value of assets that have been misappropriated from a country until these assets can be repatriated. Monetary Penalties for Breaches of Financial Sanctions. (Source: Office of Financial Sanctions Implementation HM Treasury.

8 POLICY COMPLIANCE AND CUSTODIAN

The purpose of this policy (the “Policy”) is to set out the responsibilities of RV INTERNATIONAL FZCO and all employees in observing our commitment to the avoidance Targeted Financial Sanctions Related to Terrorism, Terrorism Financing and Proliferation Training. In developing the Policy, RV INTERNATIONAL FZCO have made reference to the meet the Targeted Financial Sanctions Related To Terrorism, Terrorism Financing And Proliferation Training obligations when they qualify as DNFBPs as defined in the Cabinet Decision No.10 2019 concerning the Implementing Regulation of the AMLCFT Law (“New Sanctions Regulations”) which is repealed by Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing. As per the Cabinet Decision for Responsible Sourcing of Precious Metals and the LBMA (The London bullion market) Responsible Sourcing and Good Delivery Rules.

This Policy shall be complied with by all “Covered Persons”, namely (a) RV INTERNATIONAL FZCO, (b) all of its majority owned and controlled subsidiaries, associates, businesses or entities and (c) to all actions by their employees and shareholders. It covers dealings and transactions in all countries in which RV INTERNATIONAL FZCO operates.

9 COMPLIANCE AND ENFORCEMENT OF THIS POLICY

- This Policy was approved by the owner. The owner has overall responsibility for ensuring this Policy complies with our legal and ethical obligations, and that all those under our control comply with it.
- For the purposes of this Policy, the Compliance Manager is the Corporate Secretary. The Compliance Manager has primary and day-to-day responsibility for implementing this Policy, and for monitoring its use and effectiveness.
- Management and senior staff at all levels is responsible for ensuring those reporting to them is made aware of and understand this Policy.
- Employees are responsible to comply with RV INTERNATIONAL FZCO policies and procedures and to be alert to any behavior or actions that are inconsistent with RV INTERNATIONAL FZCO policies and procedures. Employees

also are responsible for notifying its superior or manager or the Compliance Manager of any suspected bribery and corruption.

- Top Management shall be the appointed custodian of this Policy and shall be ultimately responsible for the implementation and enforcement of this Policy.

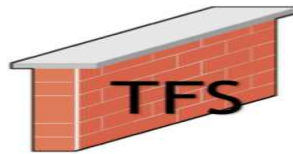
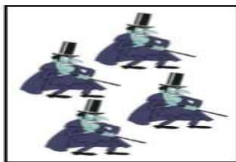
The RV INTERNATIONAL FZCO shall appoint a compliance officer who will provide expertise and assistance regarding the implementation and enforcement of this Policy thus supporting the Top Management.

10 DEFINITION - TARGETED FINANCIAL SANCTIONS

The term TFS refers to asset freezing and prohibition from making funds or other assets or services available either directly or indirectly, for the benefit of designated individuals, entities, or groups listed in the Sanctions Lists. According to the Financial Action Task Force (FATF), Targeted Financial Sanctions involve both asset freezes and prohibitions aimed at preventing funds or assets from being made available—either directly or indirectly—to designated individuals or entities.

11 WHAT IS UNITED NATIONS SECURITY COUNCIL RESOLUTION (UNSCR)?

The United Nations Security Council describes "Targeted" sanctions as those with a focused scope, directed at specific individuals, groups, or entities. Common measures include travel bans, asset freezes, and arms embargoes.



- UN Security Council – Global Policeman
- Issue binding obligatory orders to members
- Famous for imposing sanction measures on countries (and individuals)
- Financial sanction measures are relevant to Financial Institutions

12 THE FATF'S COMMITMENT TO TFS

FATF Recommendation 6 (Targeted Financial Sanctions related to Terrorism and Terrorist Financing) and 7 (Targeted Financial Sanctions related to Proliferation) required to implement the targeted financial sanctions regimes to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism and terrorist financing and proliferation/WMD and its financing.

13 FEATURES OF FATF RECOMMENDATION 6 – TFS RELATED TO TERRORISM AND TERRORIST FINANCING (SOURCE: FATF METHODOLOGY 2013)

- Countries are to identify and designate a competent authority for proposing persons/entities
- Have mechanisms for identifying targets for designation
- Standard of proof: "reasonable grounds" or "reasonable basis"
- Implement TFS without delay
- Identify DOMESTIC competent authorities to implement and enforce TFS.

14 WHAT IS PROLIFERATION FINANCING OF WEAPONS OF MASS DESTRUCTION (PF-WMD)?

- Providing funds for the rapid construction of WMD (Chemical/Biological/Radioactive/Nuclear – CBRN)
- State actors (governments) and non-state actors (individuals and organizations)
- Closely associated with science and technological research projects
- Separate UNSCRs for state and non-state actors
- Currently, North Korea (DPRK) and Iran have been designated as state actors



15 UN SECURITY COUNCIL'S APPROACH TO COUNTER TF AND PF-WMD

- UNSCR 1373 (2001) * – for local terrorists, UNSCR 1267 (1999) * – for Al-Qaida and ISIL, and UNSCR 1988 (2011) * for Taliban (CTF)
- Global approach under UNSCR 1540 (2004) and its successor resolutions (non-state actors) (CPF-WMD)
- Country-specific approach under UNSCR 1718 (2006) and UNSCR 2231 (2015) and their successor resolutions (State actors) (CPF-WMD).

16 UNSCRS WHICH ARE RELEVANT TO YOU AS FIS

- Relevant because they are associated with TFS regimes - UNSCR 1267 and related resolutions
- Al-Qaida and ISIL related individuals and entities - UNSCR 1988 and related resolutions
- Taliban related individuals and entities - UNSCR 1373 and related resolutions
- Local terrorist related individuals and entities (LTTE) - UNSCR 1718 and related resolutions
- North Korea related individuals and entities – State Actors - UNSCR 2231 and related resolutions
- Iran related individuals and entities – State Actors - UNSCR 1540 and related resolutions
- Individuals and organizations (no list!) – Non-state Actors

17 LEGISLATION ON FINANCIAL

The DNFBPs shall be without delay.

- Freeze all the funds held by it in the name of a designated entity.
- Inform the Attorney-General and the Financial Intelligence Unit that a designated entity has funds with the DNFBPs providing all details of such funds; and
- Inform the designated entity that the funds held at the DNFBPs have been frozen.

18 THE OBLIGATION TO FREEZE 'WITHOUT DELAY' DEFINED

The Glossary of the FATF Recommendations defines 'without delay', with respect to the Al-Qaida/Taliban sanctions regimes, as ideally, within a matter of hours of a designation by the United Nations Security Council or its relevant Sanctions Committee (e.g. the 1267 Committee, or the 1988 Committee). For the purposes of resolution 1373(2001), the term without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organization. In both cases, the term without delay should be interpreted in the context of the need to

prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organizations, and those who finance terrorism.

19 PROTECTION AGAINST LIABILITY FOR REPORTING PERSONS

The TFS Law and the AML-CFT Decision provide Designated Non-Financial Businesses and Professions, as well as their board members, employees and authorized representatives, with protection from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the Competent Authority.

20 THE FINANCING OF TERRORISM

In a 2019 report by MENAFATF, a sobering assessment of the global threat posed by the financing of terrorism stated:

“The number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve. Recently, the nature of the global terrorism threat has intensified considerably. In addition to the threat posed by terrorist organizations such as ISIL, Al-Qaeda and other groups, attacks in many cities across the globe are carried out by individual terrorists and terrorist cells ranging in size and complexity. Commensurate with the evolving nature of global terrorism, the methods used by terrorist groups and individual terrorists to fulfill their basic need to generate and manage funds is also evolving.

Terrorist organizations use funds for operations (terrorist attacks and pre-operational surveillance); propaganda and recruitment; training; salaries and member compensation; and social services. These financial requirements are usually high for large terrorist organizations, particularly those that aim to, or do, control territory.

In contrast, the financial requirements of individual terrorists or small cells are much lower with funds primarily used to carry out attacks. Irrespective of the differences between terrorist groups or individual terrorists, since funds are directly linked to operational capability, all terrorist groups and individual terrorists seek to ensure adequate funds generation and management.

The AML-CFT Law designates the financing of terrorism as a criminal offence, which is not subject to the statute of limitations. It defines the financing of terrorism as:

- ✚ Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by a terrorist organization or terrorist person or intended to finance a terrorist organization, a terrorist person or a terrorism crime, even if it without the intention to conceal or disguise their illicit origin; or
- ✚ Providing, collecting, preparing or obtaining proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense, or committing such acts on behalf of a terrorist organization or a terrorist person while aware of their true background or purpose.

21 SANCTIONS

A sanction is a preventative measure often implemented by governments and international bodies to change behavior, prohibit illicit activity and curb undesirable actions by certain high-risk persons or groups.

21.1 WHAT IS A SANCTIONS LIST?

A sanctions list is a compilation of individual sanctions that can be applied to individuals, countries, groups or companies. Sanction lists are often collated by governments or international bodies such as the European Union.

Managing sanctions risk has never been so complex

1. Sanctions Lists are evolving constantly.

As government increasingly rely on sanctions as a tool for political foreign policy, new entities are added to, and removed from sanctions lists, all of the time. Over the past 5 years, the average number of designated entities has increased significantly.

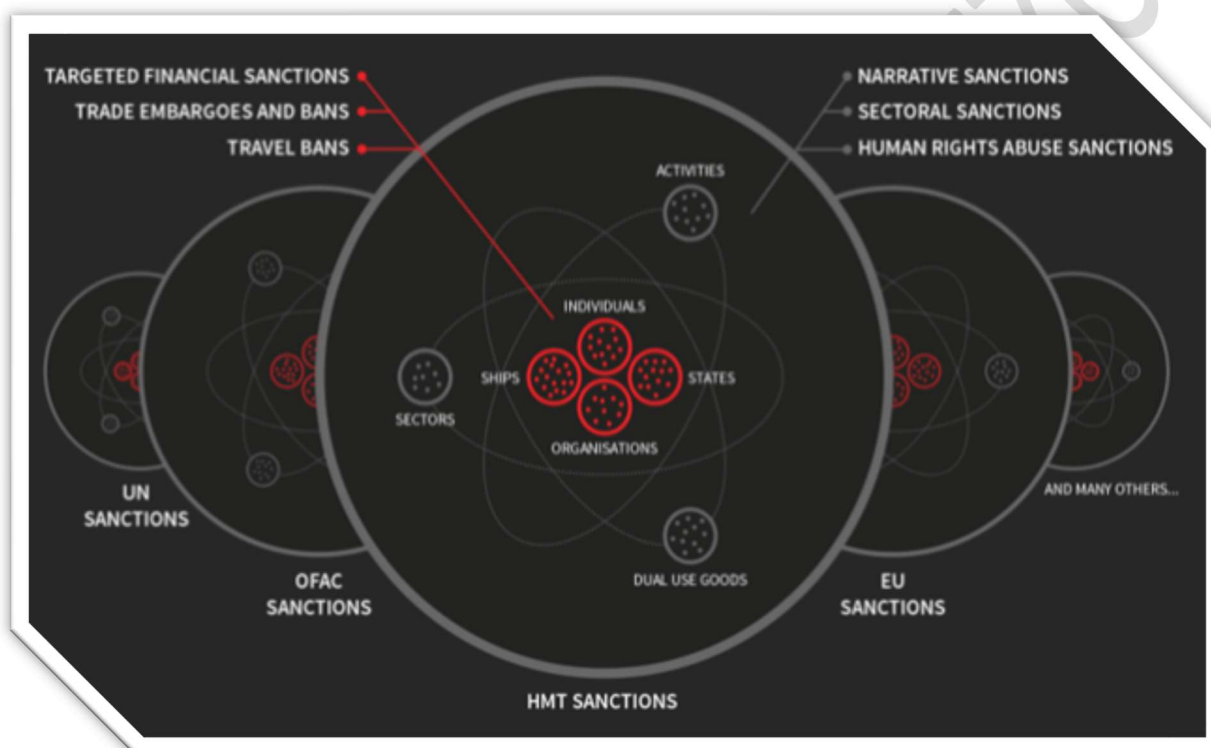
2. The nature of sanctions is becoming more complex.

Whereas they previously targeted only specific named entities (states, ships aircraft, organizations and individuals), now narrative and sectors sanctions have been introduced targeting specific sectors and prohibiting specific activities, which are more open to interpretation.

3. Sanctions aren't limited to the entities themselves.

Organizations owned or controlled by sanctioned entities also need to be in scope of sanctions lists and compliance programmes. Additionally, customers who aren't on a sanctions list but have a relationship with a sanctioned entity could also present a risk.

There are multiple sanctioning bodies with their own sanction's lists. The multitude of sanctioning bodies, including sovereign states, regional unions and international organizations such as the UN, each publish their own sanctions – which don't always align.



The relevant sanctioning bodies are:

For UK businesses, the most relevant sanctioning bodies include the European Union, HM Treasury, US Office of Foreign Assets Control (OFAC) and the UN Security Council. Beyond these, companies may also need to consider other sanctioning bodies depending on the territories, in which they trade, the currencies they trade in, and their partnerships and alliances.

1. HM Treasury Sanctions List:

The UK consolidated list of financial sanctions targets applies to:

- All individuals and legal entities who are within or undertake activities within the UK's territory.
- All UK nationals and legal entities established under UK law, including their branches (irrespective of where their activities take place)
- Office for Financial Sanctions implementation (OFSI) is responsible for ensuring UK sanctions are implemented.
- All individuals and legal entities that are within or undertake activities within the UK's territory.

- All UK nationals and legal entities established under UK law, including their branches (irrespective of where their activities take place).
- Office for Financial Sanctions implementation (OFSI) is responsible for ensuring UK Sanctions are implemented and enforced.

2. OFAC Sanctions List

The specially designated nationals and blocked persons list (SDN) applies to:

- All US citizens, wherever they are in the world.
- Corporate entities constituted in the US.

Any entity that:

- Trades in US dollars
- Uses US goods or components.
- Has a US parent, subsidiary or affiliate.
- And/or work through a local agent
- Corporate entities constituted in the US.

Any entity that:

- Trades in US dollars
- Has a US goods or components.
- Has a US parent, subsidiary or affiliate.
- And /or work through a local agent or supplier with a US connection.

3. EU Consolidated List of Sanctions

- The EU consolidated list of sanctions applies to:
- All EU citizens, wherever they are located in the world.
- Corporate entities constituted in a member state.

4. UN Sanctions

The United Nations Security Council sanctions list applies to:

- All UN Nation states.
- Companies and industry sectors need to screen for sanctions.
- All businesses in all sectors are obliged to comply with sanctions screening requirements, and therefore need to have adequate controls in place. Historically, enforcement actions have been more prominent in Financial Services, but other sectors have also received significant fines, and some regulatory bodies are increasingly turning their attention to other industries.
- For example, the Office of Financial Sanctions implementation (OFSI) has published financial sanctions guidance for charities and non-governmental organizations. Failure to comply with sanctions or obtain the correct license, in the case of export controls, can lead to significant fines. In 2019, U.S. OFAC's enforcement penalties alone hit a record U.S.\$1.2 billion. View this guide to U.S. OFAC sanctions for more detail on whether your business is in scope and how not to breach OFAC sanctions.
- It's not just customers who present sanctions risk
- Enforcement agencies can levy fines not just for sanctions violations, but also failure to have adequate controls in place. This means firms must ensure that they carry out effective sanctions screening, not only on direct third parties, but also their associates, beneficial owners and the extended supply chain, particularly in geographies known to have strong links to sanctioned countries.



21.2 HOW DOES SANCTIONS SCREENING WORK?

Sanctions screening involves screening individuals, groups or companies against designated sanction lists according to the territories in which an organization trades, the currencies they trade in, and their partnerships and alliances. This can take the form of manually inputting a name into an online search tool, checking a customer database for any sanctions alerts en masse, or automatically screening customer and stakeholder databases regularly.



21.3 WHEN SHOULD SANCTIONS SCREENING BE PERFORMED TO ENSURE SANCTIONS COMPLIANCE?

Compliance needs to be able to keep pace with the ever-changing sanctions landscape to stay compliant. To manage sanctions risk effectively, organizations need to screen their customers (both existing and new) and payment transactions against multiple sanctions lists, which can be a challenge, particularly where volumes are high.

Sanctions screening should be a top priority after the initial risk assessment when boarding a customer or third party. In addition, companies should ensure existing customers, and third parties are screened on a regular basis to maintain compliance against the dynamic and ever-changing financial and trade sanctions landscape. Possible matches should be addressed urgently, with clearly defined processes for escalation. All firms must have clearly defined senior management responsibility for sanctions compliance, since regulatory authorities are now applying much deeper levels of scrutiny to controls and procedures than ever before.

21.4 SANCTIONS SCREENING CHALLENGES

The real challenge for many companies is not just to detect customers who are on sanctions lists and prevent them from transacting with the business, but also to avoid disrupting the customer journey for legitimate customers and undermining the efficiency of the company's operations.

Key challenges include:

1. Under or over screening

If organizations do not screen robustly, there is a danger of 'false negative' where entities subject to sanctions slip through the net.

Conversely, over-screening can result in organizations generating high volumes of 'false positives'. Where non-sanctioned entities are flagged as potentially sanctioned. These false positives need time and resources to remediate to confirm they are sanctioned.

A screening engine must be capable of precision tuning to reflect the company's risk exposure and screening rules, as well as being able to deal with imprecise or inaccurate data. Machine learning technology can be used to automate the routine elimination of false positives.

2. Equivalence

Whilst previously commonplace, relying on a third party for sanctions, compliance or 'equivalence' is no longer acceptable. For example, banks historically relied on the sanctions screening controls of their correspondent banks for mutual customers. Firms should seek the advice of their professional advisers, where appropriate.

3. Divergence

In certain cases, the economic sanctions applied by different sanctioning bodies are inconsistent. For example, with Iranian sanctions, OFAC and the EU have a different stance – OFAC has decided to reinstate sanctions against Iran, whilst the EU is still providing sanctions relief and encouraging EU businesses to engage with Iran.

When transacting with an entity sanctioned by one body but not another, you should exhibit extra caution and implement additional controls.

Tips for effective sanctions screening

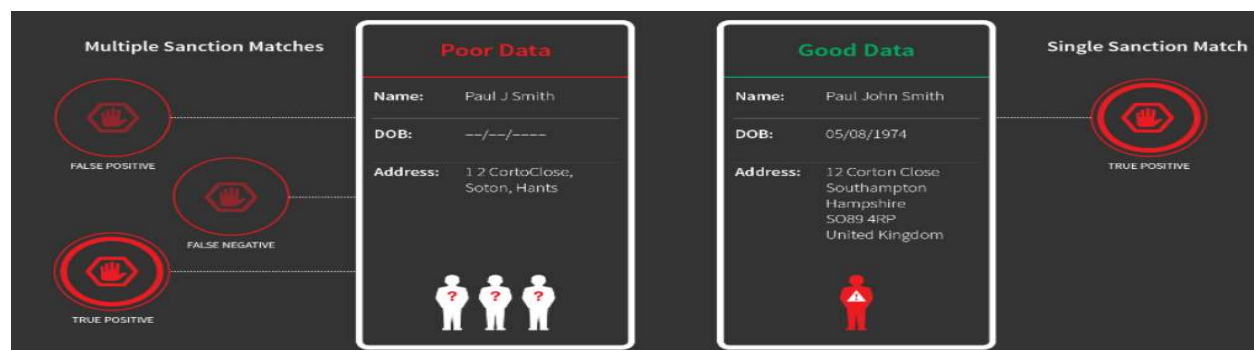
1. Prepare your customer data well:
2. Financial crime compliance costs have escalated, requiring greater focus on operational efficiency in KYC/AML. Streaming data acquisition processes, creating common data lakes and investing in enriching customer and third-party data, are highly recommended.
3. Use proven, reliable technology to support sanctions screening.
4. Solutions should be capable of handling multiple lists, batch screening, and be able to set up predefined searches tailored to an organization's risk exposure and policies.
5. Screen against high quality and comprehensive sanctions data.

Screening activities should draw from extensively researched and continuously updated global risk information incorporating the latest PEP and sanctions lists, adverse media and enforcement records from around the world.

Sanctions Screening Tip 1:

- Prepare your customer data well.
- It's critical that customer data is up-to-date and it's worth investing time to cleanse and prepare data. Incomplete or inaccurate data will result in false positives and when companies are screening millions of customers daily, this can become a real problem.
- Where possible, it is prudent to use data enrichment software to append secondary identifiers, such as date of birth, address and nationality for individuals, or business address and registration number for companies. This will help

screening platforms to focus results and will greatly improve process efficiency, saving time in unnecessary remediation, which can take up to 18 hours for a single match.



Sanctions Screening Tip 2:

- Use proven, reliable technology to support screening.
- It's important to ensure that the sanctions screening software you use to support your screening is fit for purpose. Here are some of the key considerations you should take into your account. Capacity to handle high volumes and to scale for business growth.
- The sanctions screening software you use to support your sanctions checks has to be both stable and scalable, enabling you to screen the volumes of customers and transactions that your business requires. For many companies, this will amount to millions of records daily.

Does your technology provider have the resources and infrastructure to ensure your screening and onboarding systems are operationally resilient in the long term?

User-friendly with customizable settings.

- The technology platform should be easy to use and offer configurable risk-based settings, so that you can void over-screening and adjust screening criteria to match your organization's risk appetite.
- The platform should also have workflow tools to manage the remediation of sanctions matches in a logical fashion.

Proven functionality and the ability to automate.

- Having industry proven functionality and the ability to automate tasks is vital, as this will help ensure the process is effortless and efficient all the way through from the initial loading of files, through to the results.

Capabilities such as fuzzy logic matching will increase effectiveness and help avoid false negative.

- An 'accept list' function is critical, so that once customers are cleared by screening, they will not be re-screened unless the data on their life changes in some way. This is particularly important when volumes of records are high, as it avoids the needless re-screening of records which have seen no change.
- Data stamp functionally ensures that any searches have an audit trail, evidencing for both regulators and internal stakeholders that adequate procedures have been followed.

Sanctions Screening Tip 3:

Screen against high quality and comprehensive sanctions data

- To ensure you are identifying sanctions from all relevant bodies, the data you screen your customers against must be comprehensive and up-to-date and, ideally, consolidated all in one place with other watchlist databases such as politically exposed person lists.
- Some businesses rely on search engines to locate such information, but this is inefficient and could leave your organization exposed to sanctions breaches and reputational risk.

For full confidence in your compliance, your data sources should:

- Be curated by a global network of experts
Full coverage of global sanctioning bodies requires multi-lingual research experts around the world to collate the information on a 24/7 basis. Whilst the data within sanctions listings must be returned as originally published, the best researchers will add value by providing additional contextual information. The same research can also apply to politically exposed persons to ensure profiles are fully substantiated.
- Offer a consolidated view of global sanctions lists
An individual or business could be listed on any number of the multitude of sanctions lists. Consolidating all associated sanctions listings into a single view could improve efficiencies and help avoid missing any sanctions.
- Conversely, screening against data taken solely from the relevant authority may be more efficient – consider whether your data source offers both options.

Optimize sanctions records

Sanctions lists come in a variety of formats and sizes. Being able to view them in a standardized fashion, whilst retaining the original data as published, can enhance the sanctions review process.

Add and update sanctions lists as soon as possible.

Sanctions listings are always changing, with new sanctions being added and existing ones amended or retracted. Being aware of change at the earliest possible opportunity following a sanctions notice is critical.

21.5 CUSTOMER SCREENING

Screening processes should be conducted at various stages of the customer lifecycle to include:

Periodic name screening: A change to either the customer identifying information or UN Consolidated List /Local Terrorist List should trigger an automatic rescreening.

Ad hoc name screening: Such screening is triggered by a specific business need or in order to comply with a request by a competent authority, or in the case of feedback from a downstream financial institution.

Re-screening: A specific scenario in the transaction monitoring system identifies a high-risk jurisdiction in updated customer information.

21.6 NAME SCREENING

In addition to the regular screening utilizing the UN Consolidated List and Local Terrorist List indicated above, company should maintain the following sanctions compliance procedures to prevent and detect sanctions breaches:

Ownership/Control Rule: Individuals or legal entities that are directly or indirectly owned or controlled mainly or fully by one or more Listed Person are subject to the same prohibitions as the Listed Person, even if such individuals or legal entities are not specifically named by the competent authority on the respective UN Consolidated List or Local Terrorist List.

The criterion to be taken into account when assessing whether an individual or legal entity is mainly owned by a Listed Person is the possession of more than 50% of the proprietary rights of an entity or having majority interest in it. If this criterion is satisfied, it is considered that the individual or legal entity is owned by a Listed Person.

The criteria to be taken into account when assessing whether an individual or legal entity or arrangement is mainly controlled by a Listed Person, alone or pursuant to an agreement with another shareholder or other third party, include the following:

- Having the right to appoint or remove a majority of the members of the administrative or management body of such a 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;
 - 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 exercise the right to exercise a dominant influence referred to in the previous point, without being the holder of that right;
 - Having the right to use all or part of the assets of that legal person, entity, group or arrangement;
 - Managing the business of that legal person, entity, group or arrangement on a unified basis, while publishing consolidated accounts; or
 - Sharing jointly and severally the financial liabilities of legal person, entity, group or arrangement, or guaranteeing them.
- Fuzzy Matching: An algorithm-based technique to match one data point, where the contents of the information being screened is not identical, but its spelling, pattern or sound is a close match to the contents contained on a list used for screening.
 - Weak or Low-quality Aliases: Relatively broad or generic alias may generate a large volume of false hits when such names are run through a computer-based screening system. LFI should perform their own assessments on whether to screen for weak aliases based on their understanding of their own risk profile.

21.7 VERIFICATION OF FALSE POSITIVES

Because many names may be common, various potential matches may be found. A potential match is when there is any match between data in the sanctions lists with any information in the company databases. However, it does not necessarily mean that the individual or entity the company is dealing with is subject to sanctions. When identifying the potential match, the company should suspend any transaction until they are satisfied it is not a Listed Person.

Company should compare potential matches with the UN Consolidated List and the Local Terrorist List in order to confirm whether they are true matches and to eliminate “false positives.” The company should compare information that is known about the party in question, such as date of birth and address, with other information provided in the designation order. Furthermore, company should undertake efforts to obtain additional information and identification documents, which may have previously not been obtained from the customer or a counterparty to ascertain whether the customer is the actual designated person in the case of similar or common names.

If the company establishes that the match is a false positive, then the company does not need to freezing or apply Other Measures related to sanctions. Therefore, the company may allow the transaction or relationship to continue its normal course, provided that the transaction or relationship is not suspicious and does not trigger any other concerns. The company is required to maintain evidence of the false positive verification process in their records and make them available to the competent authorities immediately upon request.

Company may create a “whitelist” (or a “good customer list”) of names of customers that have been flagged as potential matches to the UN Consolidated List and the Local Terrorist List but subsequently cleared through thorough due diligence by the company. Those “whitelists” may be used to improve the process related to screening by leveraging the results of past due diligences and reducing the number of false positives. While a company should not overly rely on such a list and must diligently and continuously screen customers and transactions in case they are implicated in updated UN Consolidated List and Local Terrorist List, the use of such a “white list” may assist the company in expediting the dispositioning in case of repeated false

positive matches. Company should have documented procedures to managing and periodically reviewing and updating those “white lists”.

21.8 PAYMENTS SCREENING

The company should also screen information regarding counterparties of all incoming and outgoing transfers in order to identify any potential match to Listed Persons. The information to be screened includes:

- The parties involved in a transaction, including the sender and the receiver
- Third parties and intermediaries
- Bank Names, Bank Identifier Code (“BIC”) and other routing codes
- Free text fields
- International Securities Identification Number (“ISINs”) or other risk relevant product identifiers (there are multiple fields in the identifier information section for sanctions lists. An ISIN number can be screened as an identifier number similar to a date of birth/passport number, and towns/regions can be screened as jurisdictions operating in).
- Geography, including addresses, countries, cities, towns, regions.

21.9 CONFIRMED MATCH

Under Articles 15 and 21 of Cabinet Decision 74, when a match is found through the screening process, the company must immediately, without delay and without prior notice, freeze all Funds.

Without delay, as defined by Article 1 of Cabinet Decision 74, means within 24 hours of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.

21.10 NOTIFICATION TO EXECUTIVE OFFICE

Under Article 21(5) of Cabinet Decision 74, LFIs must immediately notify the EO in the following cases:

- Identification of funds and actions that have been taken as per requirements of Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Terrorist List (including but not limited to freezing), including attempted transactions
- Detection of any match with Listed Persons or entities, details of the matched data, and actions that have been taken as per the requirements of Relevant UNSCRs and Local Terrorist Lists, including attempted transactions.
- Identification of a previous customer or an occasional customer listed on the UN Consolidated List or Local Terrorist List.
- Suspicion that a current or previous customer, or a person with whom they have a business relationship, is a Listed Person or has a direct or indirect relationship with a Listed Person.
- No action has been taken due to a false positive and the inability to dismiss a false positive through available or accessible information (i.e. given insufficient information, such as matching identifier information, address, DOB, or nationality).
- Unfreezing of Funds, identifying the information relating to funds that have been unfrozen, including their status, nature, value and measures that were taken in respect thereof, and any other information relevant to such decisions.

Under Article 15(2) of Cabinet Decision, LFIs must also notify the Executive Office of any freezing measures and/or attempted transactions.

According to the Executive Office’s Guidance on Targeted Financial Sanctions for FIs and DNFBPs, LFIs should notify the Executive Office within two (2) business days from taking any freezing measure and/or attempted transactions. For the reporting mechanism and form(s), please consult the Executive Office’s websites as updated from time to time.

22 RED FLAG INDICATORS/SUSPICIOUS INDICATORS

A suspicious transaction includes any activity which does not fit with the normal course of business. Few indicators can be noted as below:

- The customer does not cooperate in answering questions and refuse to give supporting documents pertaining his transactions.
- Customer who cannot provide ID when requested with the obvious intention to hide his identity.
- Politically exposed person, their family and staff.
- Cash brought in from countries with a high level of corruption or political instability.
- Transaction is not in line with the customer's business activity listed in their trade license.
- Pattern of transactions has changed since business relationship was established.
- Customer is reluctant, unable or refuses to explain:
 - their business activities and corporate history;
 - the identity of the beneficial owner;
 - their source of wealth/funds; - why they are conducting their activities in a certain manner;
 - who they are transacting with;
 - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- The customer under investigation has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.
- Refuses to cooperate or provide information, data, and documents usually required to facilitate an audit, or is unfamiliar with the details of the company's business.
- Makes unusual requests with the company or its employees.
- Appears very concerned about or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Attempts to improperly conceal beneficial ownership from competent authorities.

Red Flag Indicators for TF and PF

Accurately identifying and assessing the TF and PF risks of a customer or business relationship is critical for appropriately managing these risks.

A single indicator on its own may seem insignificant, but when combined with others it could provide reasonable grounds to suspect that the transaction is related to TF or PF activity.

Red Flag Indicators for TF

Potentially Suspicious Activity That May Indicate Terrorist Financing Published in the FFIEC BSA/AML Examination Manual.

Activity Inconsistent with the Customer's Business:

- 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).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown, or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers:

- 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 are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- 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.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- 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.

Other Transactions That Appear Unusual or Suspicious:

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- 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.
- Banks from higher-risk locations open accounts.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.
- Terrorist Financing Indicators Published by FINTRAC (Canada's Financial Intelligence Unit)
- 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.
- 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 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.
- Law enforcement information provided which indicates individual(s) or entity (ies) may be 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.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowd funding initiative, charity, non-profit organization, non-government organization, etc.).

Red Flag Indicators for PF

Indicators of Possible Proliferation Financing as mentioned in Annex 1 to the 2008 FATF Typologies Report on Proliferation Financing

- 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 shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- Transaction involves possible shell companies (e.g. companies do not have a high level of capitalization 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.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- 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.
- 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.

Red Flag Indicators for Potential Sanctions Circumventions

Some Red Flags or Situations to Identify Potential Sanctions Circumventions Published in the Executive Office’s “Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction”

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

Dealings in sectors vulnerable for terrorist financing and/or proliferation of weapons of mass destructions, for example

- Financial sector
- Hawalas or other money transfer services providers
- Oil and gas sector
- Non-profit organizations
- International trade
- Dealings, directly or through a client of your client, with high-risk countries for terrorism financing.
- 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 dual-used goods.
 - Dealings with controlled substances.
- Identifying documents that seemed to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- Use of intermediaries.
- 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 at providing 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.

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.

23 SANCTIONS COMPLIANCE PROGRAM

RV INTERNATIONAL FZCO will take appropriate steps to develop, implement and regularly update an appropriate Sanctions Compliance Program (SCP) in order to fulfill their obligation to comply with the provisions of the Cabinet Decision 74 as well as with the directives of the relevant competent authorities and supervisory authorities in regard to sanctions issued by the UNSC. An appropriate SCP also assists companies to manage their exposure to the risks associated with international financial sanctions programs and restrictive measures implemented by other countries.

RV INTERNATIONAL FZCO design and update their SCP so that its scope is proportionate to the level of their risk profile, tailored to their nature, scale, and complexity, appropriate for the products and services they offer, the customers, clients, and partner relationships they maintain, and the geographic regions in which they operate.

Company will ensure the SCP includes the eight (8) essential components: senior management commitment, risk assessment, sanctions risk appetite, internal controls, policies and procedures, training, independent audit and testing of processes and systems, and record keeping.

24 EO IEC'S ROLE

- Act as a central authority to ensure implementation of Targeted Financial Sanctions in the UAE.
- Receive and process grievances against listing in UN Consolidated List and Local Terrorist Lists decisions.
- Receive and process applications to use frozen funds as per Sanctions Lists.
- Work closely with the Supreme Council for National Security with regard to the local listing.
- Circulate updates to the Local Terrorist List and UN Consolidated List to the government and private sector.
- Coordination and exchange of information between government agencies.

25 SENIOR MANAGEMENT COMMITMENT

- Senior management is defined broadly to include senior leadership, executives, and the board of directors. Senior management's commitment to and support the SCP, the most important factors in determining its success. In order to facilitate effective senior management commitment, company will:
- Ensure that senior management has reviewed and approved the organization's SCP.
- Ensure that senior management has reviewed and approved the methodology used for undertaking the risk assessment and reviewed and approved the risk assessments at least on an annual basis.
- Clearly designate the personnel responsible for ensuring proper implementation of the SCP, including day-to-day operations, and compliance with statutory obligations. These personnel should have the appropriate competencies and experience, or be appropriately trained, to perform the duties and responsibility associated with this role, has sufficient seniority, and is delegated sufficient authority and autonomy in order to discharge the company responsibilities. The personnel may have other responsibilities in the company, provided that these responsibilities do not conflict with their role in implementing the SCP.
- Ensure the existence of direct reporting lines between the personnel responsible for the SCP and senior management to facilitate the escalation of financial sanctions issues, including regular and periodic meetings.
- Ensure that the SCP is fully integrated into the organization's daily operations and allocated adequate resources in the form of human capital, expertise, information technology, and other resources as appropriate.
- Recognize compliance failings and implement necessary measures to reduce future incidents, including through addressing root causes and implementing systemic solutions.

26 RISK ASSESSMENT

RV INTERNATIONAL FZCO will take appropriate steps to conduct a regular and updated risk assessment to identify, understand, assess, monitor, and manage their risks in line with their business nature and size. While there is no "one-size-fits all" risk assessment, the assessment exercise should generally consist of a holistic review of the company from top-to-bottom and assess its touch points to the outside world where the company may potentially, directly or indirectly, be exposed to sanctioned parties or transactions. In most cases, companies should consider performing such risk assessments annually; however, assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. These may include a change to the company risk profile, regulatory or law enforcement advisories, or global trends in terrorism financing ("TF") and the financing of proliferation of weapons of mass of mass destruction ("PF").

- In determining potential risks, company should take into account, to the extent relevant, any vulnerabilities relating to:
- its customers, supply chain, intermediaries, and counterparties;
- its products and services, including how and where such items fit into other financial or commercial products, services, networks, or systems;
- the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counterparties;
- its distribution channels and business partners;
- the complexity and volume of its transactions;
- the development of new products and business practices including new delivery mechanisms, channels, and partners;
- and

- The use of new or developing technologies for both new and pre-existing products and services.
- Company should document risk assessment operations, maintain them up-to-date on an on-going basis, and make them available upon request.
- The results of a risk assessment are integral to informing the SCP's policies, procedures, internal controls, and training in order to effectively mitigate risks.

Companies should develop and thoroughly document their risk assessment methodologies to identify, analyze, and address relevant risks. The methodologies should reflect the conduct and root cause of any violations or systemic deficiencies identified.

In 2020, the UAE undertook a TF risk assessment to broaden the scope of the TF risk assessment conducted in 2018 and to significantly deepen the UAE's risk understanding in this area. In contrast to the 2018 TF RA, the 2020 version involved participation by a broad range of stakeholders and is based on the analysis of a much wider set of data and information sources, and not limited in scope to any given number of terrorist organizations but focused instead on TF risks in general, considering the specific factors that characterize TF threats and vulnerabilities in the UAE's context through different risk scenarios. The UAE's domestic risks as well as its status as an International Financial Centre were the main perspectives through which the TF RA was conducted. The risks of the UAE being used for (1) collection, (2) movement, and (3) use of funds for terrorism purposes were considered and rated separately as advised by the FATF in the Terrorism Financing Risk Assessment Guidance 2019.

The following table provides a summary of the findings on the various individual TF risk scenarios that were analyzed, and the respective inherent risk, mitigating measures, and residual ratings.

	Risk Scenario	Inherent Risk	Mitigating Measures	Residual Rating
1	Fundraising Through social media	M-H	S	M-L
2	Crowd funding	M-L	S	L
3	Fundraising Through Virtual Currencies	M-H	M	M-H
4	Donations/Non-Profit Organizations	M-H	S	M-L
5a	Trade Activities in the UAE - Selling of goods by terrorists or terrorist networks	H	M	H
5b	Trade Activities in the UAE - Purchase of Goods or Services by terrorists or terrorist networks	H	M	H
5c	Trade Activities by terrorist or terrorist networks using UAE Legal Entities	H	M	H
6	Funds Transfers to/from High-Risk Jurisdictions	H	S	H
7	Ownership or Control over UAE Financial Institutions or MVTs	M-H	S	M-L
8	Smuggling or Transportation of Cash, including through FTFs	H	M	H
9	Investment of or Financial Management of terrorism related funds in the UAE	H	M	H
10	Terrorist Attacks in the UAE	M-H	S	M-L

Ratings: Strong (S), High (H), Medium-High (M-H), Moderate (M), Medium-Low (M-L), Low (L)

The above-mentioned risk scenarios were then subsumed under the three FATF-identified terrorism funding methods, to identify the extent of the UAE's residual risk for each. The findings are as follows:

Funding Method	UAE's Residual
1 - Collecting terrorism related funds in the UAE	Medium - Low
2 - Moving terrorism related funds through the UAE	High
3 - Using terrorism related funds in the UAE	Medium
OVERALL	Medium - High

Overall, the new TF RA's analysis demonstrates the wide range of risks the UAE faces in the context of TF, the need for the country to continue strengthening its risk mitigation measures, and the UAE's deep commitment to playing an active and key role in the global fight against terrorism and proliferation financing.

27 SANCTIONS RISK APPETITE

- Company should develop and maintain a comprehensive written sanctions risk appetite approved by the company senior management and embedded through policies, procedures, and screening systems parameterization.
- The sanctions risk appetite should specify which sanctions regimes are applicable to the LFI (for example UNSCR, OFAC, EU, UK etc.)
- Company should specify their policy on treating of interests, properties, assets, or entities that are owned or controlled 50% or more by a Listed Person.
- Company should specify their approach on mitigating the risk of breaching of unilateral sanctions, especially in the context of sanctions that may have extra-territorial implications or the Listed Persons may or may not have a presence in UAE (for example secondary sanctions by OFAC).
- Company should specify their approach on screening of alias names such as one word synonyms, vessel names or paper based instruments.
- Company should identify and document any exceptions to sanctions risk appetite or deviations from their policies and procedures; these should be approved by senior management.

28 INTERNAL CONTROLS

- Internal controls are the mechanisms, rules, and procedures implemented to help ensure the integrity and effectiveness of a company SCP.
- As required by Cabinet Decision 74, LFIs must have appropriate internal controls in place, including the most recent publication of Targeted Financial Sanctions of the UN Consolidated List and the Local Terrorist List. Accordingly, companies must maintain strong and clear internal controls that ensure the effective implementation of their SCP, including policies, procedures, processes, and systems.
- Company should document how their processes and systems are configured in order to demonstrate that their configuration is reasonably expected to detect and manage the specific sanctions risks to which the company is exposed to and ensure transparency of any system limitations or risk-based decisions that the screening controls are not designed to detect.
- Company should establish a mechanism to ensure that, upon learning of a weakness pertaining to its SPC compliance, immediate and effective action is taken to identify compliance gaps and their root causes, including all program-related software, systems, and other technology, and remediate them by implementing systemic solutions to reduce the chances of future failures.

29 POLICIES AND PROCEDURES

- RV INTERNATIONAL FZCO should develop and maintain clear and comprehensive written policies and procedures to enable them to manage and mitigate the sanctions risks they have identified, commensurate with the nature and size of their business.
- Company should ensure that policies and procedures are approved by senior management and that they:
 - Enable the company to clearly and effectively identify, prevent, escalate, and report suspicious transactions and activities;
 - Are tailored to the organization and capture the organization's day-to-day operations and processes;
 - Are easy to follow and designed to prevent employees from engaging in misconduct;
 - Prohibit employees from, directly or indirectly, informing the customer or any third party that freezing or any Other Measures shall be implemented;
 - Require enhanced due diligence to be conducted on all customers and transactions that are assessed to be high-risk for TF and PF; and
 - Contain sufficient detail of their record keeping obligations.

- Company should ensure the effective and consistent implementation of the policies and procedures related to the SCP across their organizations, including branches, Subsidiaries, and other entities in which company hold a majority interest.
- Company should clearly communicate the SCP's policies and procedures, including for record keeping, to all relevant employees and external or outsourced service providers.
- Company should review and update policies and procedures in a timely manner in response to events or emerging risks and ensure that such updates are communicated to employees on a timely basis.
- Company should implement a formal review process at least annually of the policies and procedures at appropriate levels subject to approval where changes are material.
- Company should identify and document any exceptions or deviations from the policies and procedures related to the SCP; these should be approved by senior management.

30 TRAINING

The maintenance and implementation of an effective SCP requires that all relevant employees and management understand requirements and obligations, policies and procedures, internal control mechanisms, and threats, risks, and vulnerabilities. A robust training program is an integral component of an effective SCP. A training program should:

- Be of a scope and nature proportionate to the company overall risk profile.
- Be specific to the role carried out by the employee, with tailored training for employees engaged in sensitive roles;
- Provide training to all appropriate employees and personnel upon onboarding in a timely manner and at least annually thereafter;
- Hold employees accountable for training through assessments;
- Include measures to take immediate and effective action to provide corrective training or other corrective actions to relevant personnel upon learning of a confirmed negative risk assessment result or audit finding, or other deficiency pertaining to the SPC.

31 INDEPENDENT AUDIT AND TESTING OF PROCESSES AND SYSTEMS

Independent audit helps the LFI assess the effectiveness of current processes, including by assessing the sufficiency of the program and by checking for any inconsistencies between the policy and procedures and day-to-day operations in order to identify SCP weaknesses and deficiencies. Independent audits should:

- Be undertaken regularly to review and assess the effectiveness of the financial sanctions policies, procedures, systems and controls, and their compliance with the company obligations;
- Be undertaken by the internal audit function, or by a competent independent external auditor, or both, and resourced with skilled and competent staff that understand the SCP of the company; and
- Be commensurate to the level and sophistication of the SCP and updated to account for changing risk assessments or sanctions environments.

Company will ensure that the audit function is independent of the audited activities and functions, and has sufficient authority, skills, expertise, and resources within the organization. Company should immediately address negative audit findings and take the necessary steps to identify and implement compensating controls until the root cause is remediated.

In addition, Company will deploy an independent risk-based testing regime to regularly test their processes and systems' adequacy and expected outcomes, as well as to assess their effectiveness in managing the specific risks articulated in the risk assessment. Regular testing of processes and systems ensures that the screening application generates expected alerts, threshold settings and/or screening rules to forego or suppress undesirable alerts in accordance with the company risk appetite.

Regular testing should be supported by metrics, analysis, and reporting, and be reviewed by the personnel responsible for the SPC to determine whether risk acceptance or remediation is appropriate with respect to any relevant findings. Regular testing could be undertaken by the internal audit function, or by a competent external provider, or both.

32 RECORD KEEPING

According to the AML-CFT Law and the AML-CFT Decision, company must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as all records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed. The company must maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. Company must make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, from the date of completion of the transaction or termination of the business relationship, or from the date of completion of the inspection, or from the date of issuance of a final judgment of the competent judicial authorities, all depending on the circumstances.

33 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 member countries, 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's decisions. The UNSC holds the capacity to take any action to maintain or restore international peace and security under Article 41 of Chapter VII of the Charter of the UN 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 Countering Proliferation Financing (CPF), under Recommendations 6 and 7 (R6/R7) of the FATF Standards, requires the implementation of TFS to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention and suppression of terrorism, TF, and PF.

The UAE, as a member of the UN, is committed to implementing UNSCRs, including those related to the UN's sanctions regimes. Consequently, through Cabinet Decision No. 74 of 2020, the UAE Implements relevant UNSCRs on the suppression and combating of terrorism, TF and PF, 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 UAE Local Terrorist List in accordance with UNSCR 1373 (2001), which calls for Member States to publish their own national terrorist lists.

SECTION 1: LEGAL FRAMEWORK

The following list comprises the legislations issued for the purpose of implementing TFS in the UAE:

TITLE	ISSUED
Federal Law No. 20 for 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations and its amendments repealed by Federal Decree-Law No. 10 of 2025 Regarding Anti- Money Laundering and Combating the Financing of Terrorism, and Proliferation Financing	Issued: 2018 Amended: 2021 (Federal Law No. 26) Updated in 2025

Cabinet Decision No.10 2019 concerning the Implementing Regulation of the AMLCFT Law (“New Sanctions Regulations”) which is repealed by Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing	Issued: 2019 Amended: 2022 (Cabinet Decision No. 24)
Cabinet Decision No. 134 of 2025 on the Executive Regulations of Federal Decree-Law No. 10 of 2025 Regarding Anti- Money Laundering and Combating the Financing of Terrorism, and Proliferation Financing	2025
Cabinet Resolution No. 71 of 2024 on Regulating Violations and Administrative Penalties Imposed on Violators of Anti-Money Laundering, Combating Terrorist Financing, and Proliferation Financing Procedures	2024
Cabinet Decision No. 74 of 2020 concerning the UAE 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.	2020
Guidelines, controls, circulars, and other national-level guidance issued by the Ministry and the Executive Office for Control and Non-Proliferation (EOCN), as well as any other sector-specific national guidance relevant to your entity.	

SECTION 2: TARGETED FINANCIAL SANCTIONS DEFINITION AND SCOPE

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 Sanctions Lists, immediately (within 24 hours) upon designation. 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:

For DNFBP's: A freezing measure can be stopping the facilitation of or blocking the transfer of ownership of immovable (real estate) or movable asset's (gold).

For VASP's: A freezing measure can be blocking services to trade and transfer virtual assets, as well as suspending/restricting access to accounts.

PROHIBITION FROM MAKING FUNDS OR OTHER ASSETS OR SERVICES AVAILABLE:

This means the prohibition to provide funds or other assets or financial services to any designated individuals, entities or group listed in the sanction's lists.

EXAMPLE:

For DNFBP's: The provision of any services, such as legal services to transfer asset ownership, buying or selling real estate, precious metals, natural resources etc.,

For VASP's: The provision of any virtual asset services, including but not limited to providing advisory, brokerage, custody, exchange, lending, borrowing, management, investment, transfer and settlement.

FUNDS OR OTHER ASSETS

"Funds or Other Assets" refers to any type of asset, including but not limited to financial assets and economic resources (such as oil and other natural resources), as well as all forms of property—whether tangible or intangible, movable or immovable, and regardless of how they were acquired. This also includes legal documents or instruments, whether physical, electronic, or digital, that prove ownership of or interest in such assets.

Examples include bank credits, traveler's cheques, bank cheques, money orders, shares, securities, bonds, drafts, and letters of credit. The term also encompasses any interest, dividends, or income generated from these assets, as well as any other items that could potentially be used to obtain funds, goods, or services.

CATEGORIES OF FUNDS OR OTHER ASSETS

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

FINANCIAL ASSETS

Funds and other financial assets subject to sanctions are:

- a. Cash, cheques, claims on money, drafts, money orders, bearer instruments.
- b. Deposits with FIs or other entities and balances on accounts, including but not limited to: fixed or term deposit accounts, balances on share trading accounts with banks, brokerage firms, or other investment trading accounts.
- c. Debts and debt obligations, including trade debts.
- d. Accounts receivable, notes receivable, and other claims of money.
- 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.

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:

- Land, buildings, or other real estate.
- Equipment, including computers, computer software, tools, and machinery.
- Office furniture, fittings and fixtures and other items of a fixed nature.
- Vessels, aircraft, and motor vehicles.
- Inventories of goods.
- Works of art, cultural property, precious stones, jewellery, or gold.
- Commodities, including oil, minerals, or timber.
- 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.
- 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.

ANY OTHER ASSETS

- a. Other intangible assets subject to sanctions include assets of any kind, which potentially may be used to obtain funds, goods, or services, such as patents, trademarks, copyrights, trade names, franchises, goodwill, and other forms of intellectual property, internet hosting or related services.
- b. Internet-based and other electronic or digital payment instruments, including virtual assets.

SCOPE OF TFS MEASURES

TFS measures as per UAE legislation apply exclusively on individuals, entities, and groups that are listed on the UAE Local Terrorist List, pursuant to a UAE Cabinet Decision, or the UNSC Consolidated List, pursuant to a decision by the relevant UNSC Sanctions Committee.

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 delisted (removed) from the UAE Local Terrorist List or the UNSC Consolidated List or until there is a freezing cancellation decision communicated by the EOCN.

For designations on other unilateral / multilateral sanctions lists (e.g. OFAC, UKHMT, EU, etc.), contact your Supervisory Authority (SA) on the appropriate course of action for dealing with matches on other sanctions lists.

SECTION 3: 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 proliferation. 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 as long as they remain subject to the TFS measures. TFS are implemented in the UAE pursuant to UNSCRs in relation to:

TERRORISM AND TF:

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)
4. Al-Shabaab Sanctions Committee	UNSCR 2713 (2023)

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 programs.	UNSCR 1718 (2006) and its successor resolutions
---	---

OTHER UN SANCTIONS REGIMES WITH TFS:

1. Iraq	UNSCR 1518 (2003)
2. The Democratic Republic of Congo (DRC)	UNSCR 1533 (2004)
3. Sudan	UNSCR 1591 (2005)
4. Lebanon	UNSCR 1636 (2005)
5. Libya	UNSCR 1970 (2011)
6. Guinea-Bissau	UNSCR 2048 (2012)
7. Yemen	UNSCR 2140 (2014)
8. South Sudan	UNSCR 2206 (2015)
9. Haiti	UNSCR 2653 (2022)
10. Central African Republic (CAR)	UNSCR 2745 (2024)

TFS TARGET MEASURES

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

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

Application of TFS measures on different ownership structures is explained in detail in Section 5: Ownership, Control, and Acting on Behalf of or at the Direction of Designated Individuals or Entities.

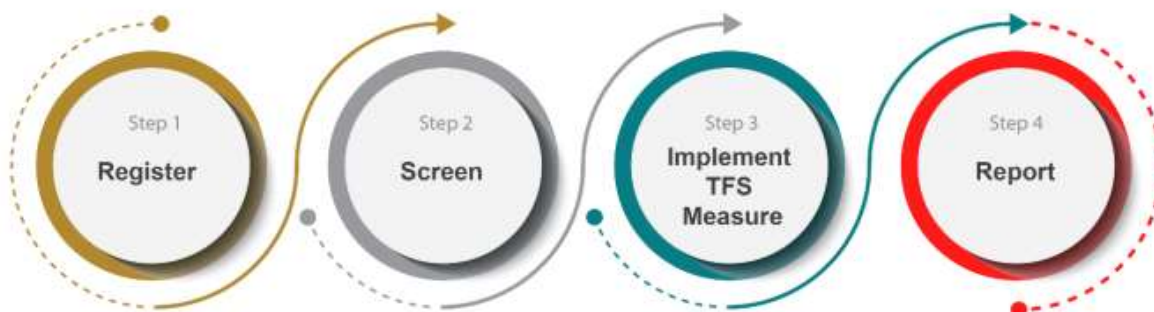
SANCTION LISTS UPDATES

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 UNSC has a UNSC Consolidated List of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC.
- The EOCN has created a subscription-based notification system, known as the EOCN Notification Alert System (NAS), which automatically sends out any updates to the Sanctions Lists to all subscribed entities.

SECTION 4: TFS OBLIGATIONS

Article 21 of Cabinet Decision 74 of 2020 has set the main TFS obligations on RV INTERNATIONAL FZCO. The four main obligations are listed below:

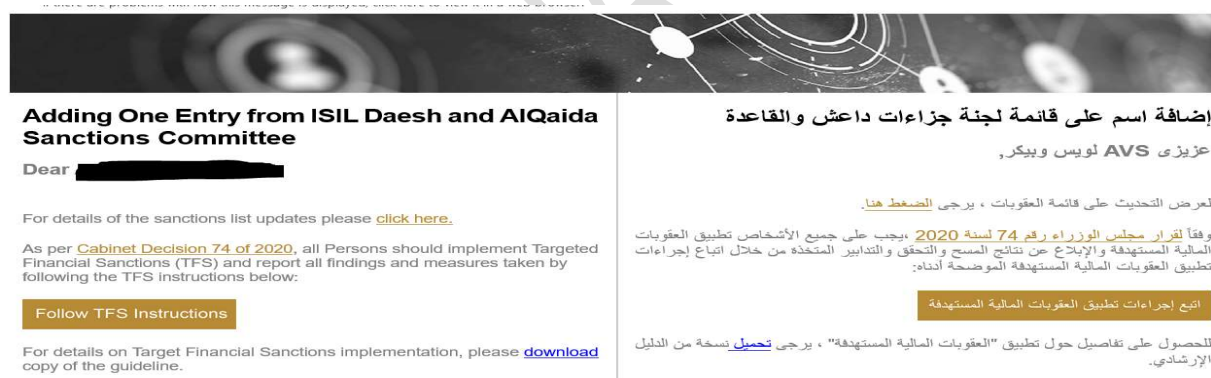


STEP 1 – REGISTER

RV INTERNATIONAL FZCO are required to register to the Notification alert system on the EOCN's website to receive automated email notifications on any updates to the sanctions list. This registration is aimed to help RV INTERNATIONAL FZCO receive updated and timely information about the designation, de-listing, or amendments of individuals, entities or groups designated in the sanction's lists.

For guidance on how to register, refer to Annex I: EOCN Notification Alert system subscription guide. "Follow TFS Instructions"

The NAS includes a "Follow TFS Instructions" feature which provides a step-by-step guide for RV INTERNATIONAL FZCO on their obligations to implement TFS as per Cabinet Decision No. 74 of 2020, including screening, freezing, and reporting.



STEP 2 – SCREEN

RV INTERNATIONAL FZCO must undertake regular and ongoing screening on the latest sanctions lists. In addition to registering on the EOCN NAS to receive alert updates, RV INTERNATIONAL FZCO should also check the UN website for press releases regularly or daily to remain vigilant on any updates to UN sanctions lists.

Screening must be undertaken in the following circumstances:

- Upon any updates to the sanction's lists, in such cases, screening must be conducted immediately to ensure compliance with implementing freezing measures without delay (within 24hrs).
- Prior to onboarding new customers.
- Upon periodic KYC reviews or if there is a material change in the nature or ownership of the customer.

- d) Daily screening of customer's databases.
- e) Before processing any transaction of a counterparty.

The Following databases must be included in the screening process:

RV INTERNATIONAL FZCO must undertake regular and ongoing screening on the latest Sanctions Lists. In addition to registering on the EOCN NAS to receive alert updates, RV INTERNATIONAL FZCO should also check the UN website for press releases regularly or daily (depending on business model) to remain vigilant on any updates to UN Sanctions Lists.

- a. Existing customer databases. If RV INTERNATIONAL FZCO uses an automated screening system, all systems containing customer data and transactions need to be mapped to the screening system to ensure full compliance. Alternatively, in the case of manual screening, RV INTERNATIONAL FZCO should ensure that their manual screening is done accurately and as per the key screening identifiers mentioned below.
- b. Potential customers before conducting any transactions or entering a business relationship with any Person.
- c. Previous customers with no current active accounts/relationship up to a period of 5 years.
- c. Names of parties to any transactions (e.g., buyer, seller, agent, freight forwarder, etc.) Ultimate beneficial owners (UBOs), both natural and legal.
- d. Names of Persons with direct or indirect relationships with designated individuals, entities or groups. f. Directors and/or agents acting on behalf of customers (including individuals with power of attorney).

The Sanctions Lists contain a range of information to aid the identification of designated individuals, entities, or groups during the screening process. It is essential to ensure that the screening is done on the key identifiers first prior to considering any other identifiers (such as "a.k.a – also known as"). If none of the key identifiers match, then the screening result is considered a "Negative Match".

The following are examples of the key identifiers:

FOR NATURAL PERSONS	FOR LEGAL PERSONS
Individual's Name Date of Birth Nationality ID or Passport Number Last Known Address	Entity or Company's Name Trade License Number Address of Registration Address of Branches

There are four possible results following the screening process, as listed below:

SCREENING RESULT	DEFINITION	EXAMPLES
CONFIRMED NAME MATCH	A Confirmed Name Match is when an individual, entity, or group matches all the key identifiers published on the UAE Local Terrorist List or UNSC Consolidated List.	Your customer's name, nationality, and DOB fully match with the identifiers of a designated Person in the UAE Local Terrorist List or UNSC Consolidated List.
PARTIAL NAME MATCH	A Partial Name Match is when there is a partial match between the key identifiers in the UAE Local Terrorist List or UNSC Consolidated List and a customer's information in your database, and you are unable to conclude a False Positive or a Confirmed Name Match.	Your customer's name and DOB match with the identifiers of a designated Person in the UAE Local Terrorist List or UNSC Consolidated List, but the nationality is different and there is a slight difference in the name spelling.
FALSE POSITIVE	A False Positive is a match to listed individuals, entities, or groups, which upon examination of key identifiers, such as full name, DOB, and nationality, proves not to be the designated individuals, entities, or groups.	Your customer's name matches with a designated Person who is 40 years old according to the DOB identifier in the UAE Local Terrorist List or UNSC Consolidated List, but your customer is a 16-year-old high school student.

Negative Match	A Negative Match is when no match is identified upon conducting screening.	You have conducted screening following a designation on the UAE Local Terrorist or UNSC Consolidated List and neither a Confirmed nor a Partial Name Match was identified.
-----------------------	--	--

CONFIRMED NAME MATCH – If it is on an existing customer, you must freeze immediately without delay, refrain from offering any funds or other assets or services and submit a Confirmed Name Match Report (CNMR) detailing the freezing measures to the EOCN and the relevant SA through the GoAML platform within five business days from taking any freezing measure. In case the Confirmed Name Match is a potential customer (a prospective client), you must reject the transaction immediately and submit a CNMR.

PARTIAL NAME MATCH – If existing client is identified in the UAE Local terrorist list or UNSC Consolidated List and a customer's information in your database and if we are unable to verify the match as confirmed or false positive then it should be considered as "Partial Name Match". In this case, you must either suspend the transaction immediately without delay, refrain from offering any funds or other assets or services or reject the transaction and submit a PNMR to the EOCN and the relevant SA through the GoAML platform within five business days from rejecting the transaction or any suspension measure taken.

FALSE POSITIVE - In case a match is identified, and upon examination of key identifiers, you're able to conclude that the match is not the designated individual, entity, or group, then the result is considered a 'False Positive'. In this case, no reporting is required; however, internal documentation on the False Positive result should be maintained.

In cases of weekends and public holidays, RV INTERNATIONAL FZCO should have appropriate internal procedures to effectively screen against the UAE Local List and the UNSC Consolidated List and prevent access or use of funds or other assets that may be subject to freezing measures. If the RV INTERNATIONAL FZCO is not conducting any business activities or transactions and where customers do not have access to any assets or accounts during weekends or holidays, then the screening obligation starts from the first minute of commencement of business and freezing measures must be applied immediately. In any case, RV INTERNATIONAL FZCO should ensure that funds or other assets subject to TFS measures are prevented from being accessed or used.

STEP 3 – IMPLEMENT TFS MEASURES

The following are the TFS measures that must be implemented if a Confirmed Name Match with the Sanctions Lists is identified:

Freeze all funds or other assets without delay:

Freeze without delay (within 24 hours) and without prior notice to the designated individual, entity or group all the funds or other assets.

- Owned or controlled, wholly or jointly, directly, or indirectly, by an individual, entity, or group designated in the Sanctions Lists.
- Derived or generated from funds or other assets under item (a); or
- 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 such as 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.

Prohibition from making funds or other assets or services available:


RV INTERNATIONAL FZCO are prohibited from providing funds or other assets to or rendering financial or other services related to, whether in whole or in part, directly or indirectly, for the benefit of any designated individual, entity, or group on the Sanctions Lists.

Lifting of freezing measures:

Freezing applied as a result of TFS measures have no time limits. Asset freeze remains valid until one of the following occurs:

- The designated Person is delisted (removed) from the Sanctions Lists. Upon delisting, all TFS measures are to be lifted immediately without prior approval from EOCN or the relevant SA, unless there is an active Freeze Order related to the delisted Person issued by a Competent Authority (FIU, Public Prosecution, etc.)
- A freezing cancellation decision by EOCN is communicated to the RV INTERNATIONAL FZCO through GoAML.

STEP 4 – REPORT

The mechanism to report any TFS measures taken upon identifying a confirmed or partial name match is through submitting one of the following via GoAML:

i) CONFIRMED NAME MATCH REPORT (CNMR):
EXISTING CUSTOMER:

RV INTERNATIONAL FZCO must freeze without delay (within 24 hours) and prohibit making funds or other assets or services available and submit a CNMR through goAML within five business days of implementing the freezing measures.

POTENTIAL CUSTOMER/COUNTERPARTY

If the party identified as confirmed name match on a potential customer ie, a prospective client then the transaction/ business with the party needs to be rejected and refrain from dealing with or providing any funds or other assets or services to the confirmed Name match and submit a CNMR report.

OBLIGATORY INFORMATION

The following information is obligatory and must be provided (attached) when submitting a CNMR:

The full name of the ‘Confirmed Name Match’.

Attach ID documents of the ‘Confirmed Name Match’, such as passport or ID card for individuals, and trade licenses and articles of association for entities. In cases of a Confirmed Name Match, it is assumed that the RV INTERNATIONAL FZCO possesses the ID documents of the confirmed match, since verifying the confirmed match result without an ID is improbable and unlikely.

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 documentary proof as bank statements, transaction receipts, securities portfolio summary, title deeds, insurance policy, etc.

Description of rejected transaction or service – (e.g. in case no funds are being held, and the transaction is service based, provide a description of the transaction / service rejected.)

PREVIOUS BUSINESS RELATIONSHIPS/TRANSACTIONS AND RECORD KEEPING

RV INTERNATIONAL FZCO are required to maintain records of all screening results (Confirmed Name Match, Partial Name Match, and False Positives) for at least five years.

CNMRs should also be reported on previous business relationships and transactions occurring and accounts held prior to the designation, covering a timeframe of five years. CNMRs should be submitted even if no current funds or other assets are held by the RV INTERNATIONAL FZCO and includes closed accounts. In this case, the RV INTERNATIONAL FZCO is required to clarify in the description of the CNMR that no funds or other assets are currently being held, and there is no current business relationship with the Confirmed Name Match, and the status of the accounts (closed) if applicable.

ii) PARTIAL NAME MATCH REPORT (PNMR)

EXISTING CUSTOMER

In case a Partial Name Match is identified on an existing customer, it is assumed that the RV INTERNATIONAL FZCO already possesses the identification documents of the customer and, after reviewing the ID documents, is unable to conclude whether the match is a Confirmed Name Match or False Positive. In this case, the RV INTERNATIONAL FZCO must suspend without delay any transaction, refrain from offering any funds, other assets or services, and submit a PNMR through GoAML within five business days from suspension measures. The Reporting Entity must ensure that all necessary information and documents regarding the Partial Name Match are submitted and maintain suspension measures until further instructions are received from EOCN via GoAML on whether to cancel the suspension ('False Positive') or implement freezing measures ('Confirmed Name Match').



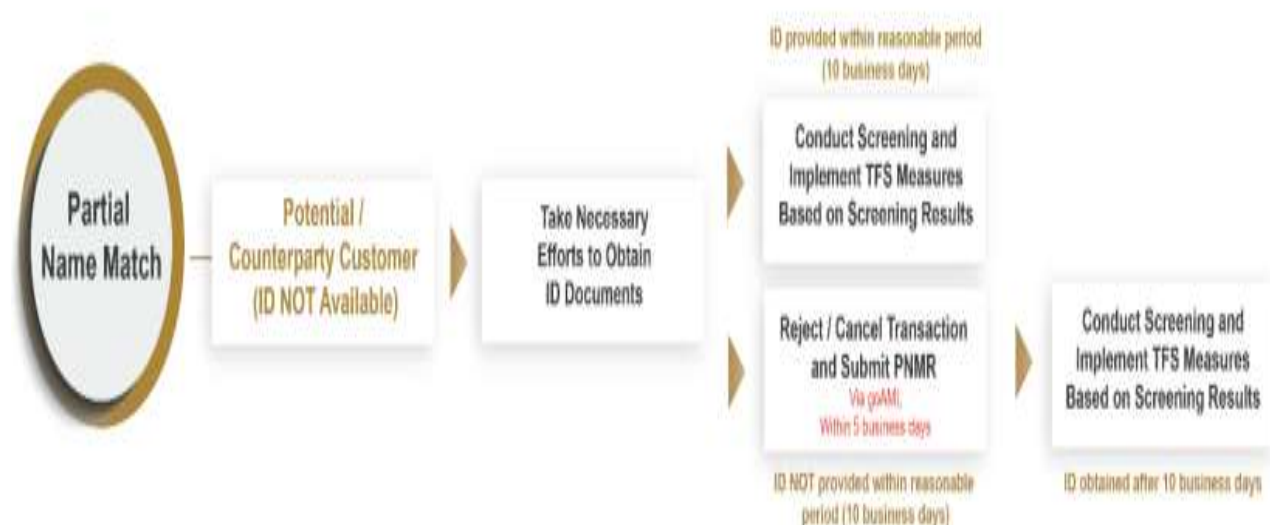
POTENTIAL CUSTOMER/COUNTERPARTY

In case a Partial Name Match is identified on a potential customer (a prospective client) or a counterparty (such as the counterparty in a bank or exchange transaction), the RV INTERNATIONAL FZCO must first make necessary efforts to obtain identification documents of the potential customer or counterparty to conclude whether the match is a Confirmed Name Match or False Positive. If, after obtaining the ID documents, the RV INTERNATIONAL FZCO is able to conclude the result as a False

Positive, then it may establish the business relation or allow the transaction to proceed without the need to report a PNMR; however, internal documentation of the False Positive result should be maintained.

If the Reporting Entity is unable to obtain the identification documents within a reasonable time (10 business days) of identifying the Partial Name Match, then the transaction or service should be rejected (cancelled) and a PNMR submitted through GoAML within five business days from rejection of the transaction or service, specifying that the transaction has been rejected due to lack of ID documents of the Partial Name Match.

If the RV INTERNATIONAL FZCO receives the ID document of the potential customer or counterparty after the transaction has been rejected due to lack of ID document (i.e. reasonable period has passed – 10 business days) and the PNMR reported, it must conduct screening based on the newly obtained ID documents and take the necessary steps required depending on the screening result (Confirmed Name Match, False Positive, or unable to verify based on the provided ID documents). In this case, the Reporting Entity may treat the case as a new transaction and submit a new report based on the screening results.



The following information is obligatory and must be provided (attached) when submitting a PNMR:

- The full name of the 'Partial Name Match'. Attach ID documents (if and when available) of the 'Partial Name Match', such as passport or ID card for individuals, and trade licenses and articles of association for entities. Note that the EOCN will not be able to verify the result of a Partial Name Match (Confirmed Match or False Positive) in the event of lack of ID documents.
- 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.
- Description of rejected transaction or service – (e.g. in case no funds are being held, and the transaction is service based, provide a description of the transaction / service rejected.)

Previous Business Relationships / Transactions and Record Keeping.

The same procedures as CNMRs apply when reporting previous business relationships, accounts, and transactions.

REPORTING TFS BY EMAIL

For non GoAML users (Persons that do not fall under the definition of Reporting Entities – Fis, DNFBPs, and VASPs – and are therefore not under an obligation to register on GoAML – these include all natural and legal persons in the UAE), the reporting of any freezing measures or attempted transaction by a designated individual, entity, or group must be communicated directly by email to the EOCN through tfs@eocn.gov.ae within five business days from implementing any freezing measures. The email

must include information on the full name of the Confirmed or Partial Name Match, and the value of frozen funds or other assets (attaching ID and documentary proof as listed above).

ADDITIONAL OBLIGATIONS FOR REPORTING ENTITIES:

In addition to the above, RV INTERNATIONAL FZCO must fulfil the following obligations:

- i. Set and implement policies, procedures, and internal controls to:
 - Ensure compliance with the obligations arising from Cabinet Decision No. 74 of 2020.
 - Adopt reasonable measures to consider beneficial owners, signatories, and powers of attorney with respect to accounts or transactions held by Reporting Entities when searching for activities by designated Persons.
 - Prohibit staff from, directly or indirectly, informing the customer or any third party that freezing action is going to be implemented as per provisions of Cabinet Decision No. 74 of 2020.
 - Ensure having the appropriate human and technical resources to meet the obligations of implementing TFS.
 - Conduct ongoing TFS training and awareness sessions to relevant employees and senior management.
- ii. Put appropriate internal controls and procedures to effectively implement TFS measures.
- iii. Cooperate with the EOCN and the relevant SA in verifying the accuracy of the information in submitted reports.
- iv. Implement the freezing and lifting of freezing measures, upon designation or de-listing respectively, without delay, pursuant to related UNSCRs or decisions of the Cabinet regarding issuance of the UAE Local Terrorist List.

SECTION 5: OWNERSHIP, CONTROL, AND ACTING ON BEHALF OR AT THE DIRECTION OF DESIGNATED PERSONS.

MAJORITY INTEREST

RV INTERNATIONAL FZCO 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.

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, RV INTERNATIONAL FZCO 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.

RV INTERNATIONAL FZCO 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.

SECTION 6: ENFORCEMENT MEASURES

CONSEQUENCES FOR REPORTING ENTITIES

Any Person, found to violate and/or be in non-compliance with the obligations stated in Cabinet Decision No. 74 of 2020 or failing to implement reasonable 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, Reporting Entities are subject to supervision, and in the case of identified non-compliance, the SA can apply the enforcement actions set out under Article (14) of Federal Decree No. 26 of 2021 Amending Certain Provisions of Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in the UAE is Federal Decree No. (20) Of 2018 On Anti-Money Laundering And Countering The Financing Of Terrorism (“Federal Decree”). This Law Has Been Repealed By The Federal Decree By Law No. (10) Of 2025 Regarding Anti-Money Laundering, And Combating The Financing Of Terrorism And Proliferation Financing. (the “AML-CFT Law” or “the Law”). The SAs of the Reporting Entities have the legal capacity to supervise the implementation of TFS.

EXEMPTION FROM LIABILITY IN CASE OF GOOD FAITH TFS IMPLEMENTATION

Any Person who, in good faith, freeze funds or other assets, or refuses to provide financial services to designated individuals, entities, or groups) 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.

I. Describe the appeal process?

The appeal process for sanction penalties does not usually take place in judicial proceedings but rather consists of the submission of grievances and other administrative proceedings. Depending on such proceedings, it may be possible in certain cases to raise a claim and to appeal a decision before the courts. The UAE does not have a binding precedent system; therefore, information regarding cases in the UAE is not always publicly available.

Criminal and civil enforcement only at the national level where there is parallel state or local enforcement.

Criminal and civil enforcement are at both the local and federal level. While the administers its applicable laws at a federal level, customs laws are often administered at a local level, for example, with respect to Dubai by the Dubai Customs Department and with respect to Abu Dhabi Customs Department.

II. The statute of limitations for economic sanctions violations.

Under Federal Law No. 5 of 1985 regarding civil transactions (“Civil Code”), the statute of limitation for civil claims is 15 years, unless otherwise expressly provided in a statute. With respect to money laundering or financing terrorism or crimes by illegal organizations, Article 29(3) of the AMLCFT Law provides that “[t]he criminal case shall be subject to the statute of limitations for money laundering or financing terrorism or illegal organizations crimes”.

SECTION 7: OBLIGATIONS REGARDING UNILATERAL / MULTILATERAL SANCTIONS REGIMES AND SANCTIONS EVASION

Reporting Entities should be able to differentiate between cases that require submitting a CNMR/PNMR, and between suspicious transactions and activities that require submitting a STR/SAR.

Any suspicious transactions or activities that might be related to sanctions evasion, and which do not include Confirmed or Partial Name Matches to the Sanctions Lists, should be reported to the FIU by raising a STR/SAR through the goAML platform.

Similarly, in case any Confirmed or Partial Name Match is identified to a unilateral / multilateral sanctions list or other criminal lists (i.e. OFAC, EU, HMT, INTERPOL, etc.), the Reporting Entity should not use the CNMR/PNMR reports in goAML to report such cases, since CNMRs/PNMRs are used to report matches with the UAE Local Terrorist List and UN List only; however, you should consult with your relevant SA on the appropriate course of action and may consider raising a STR/SAR with the FIU in case a match is identified with other sanctions or criminal lists.

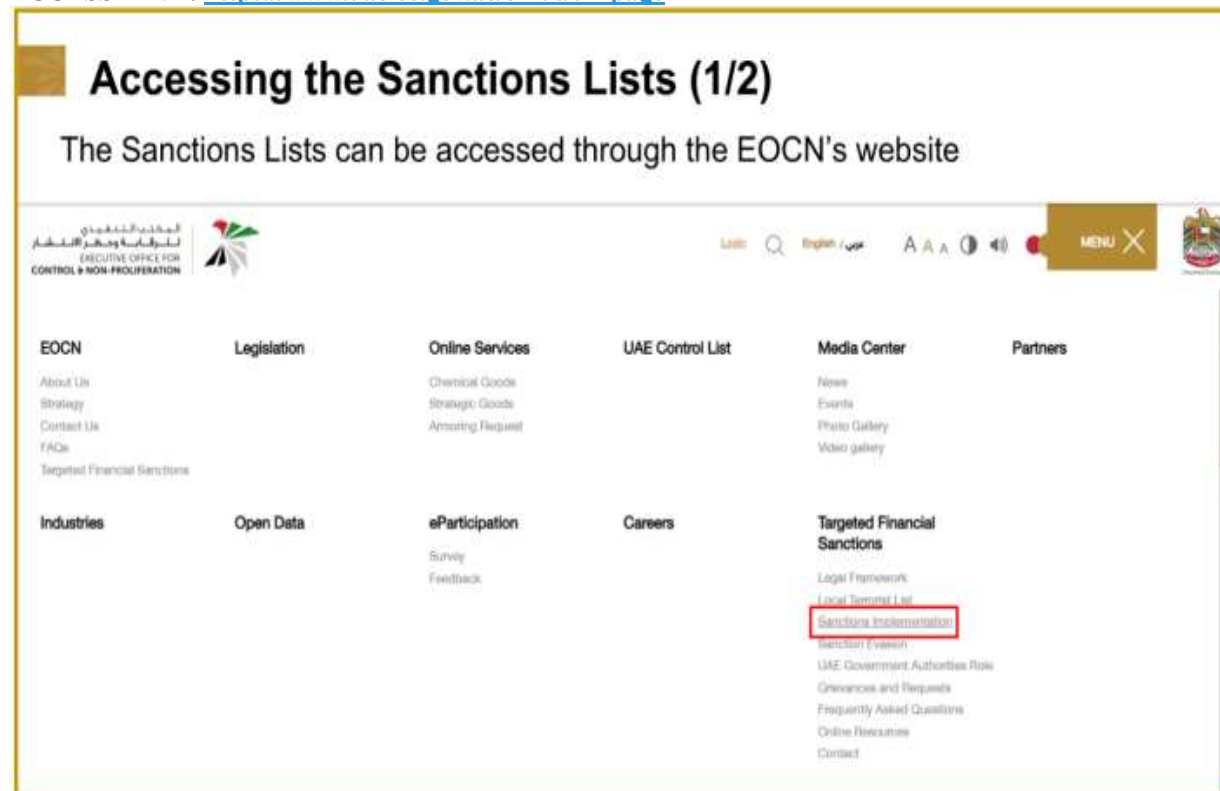
Reporting Entities are advised to familiarize themselves with the sanctions evasion related Reasons for Reporting (RFRs) in goAML when submitting a STR/SAR. For the full list of PF and TF related red flags, please refer to the Terrorist and Proliferation Financing Red Flags Guidance.

ANNEXURE I: EOCN NOTIFICATION ALERT SYSTEM SUBSCRIPTION GUIDE

ACCESS LINK: <https://www.uaecic.gov.ae/en-us/un-page>

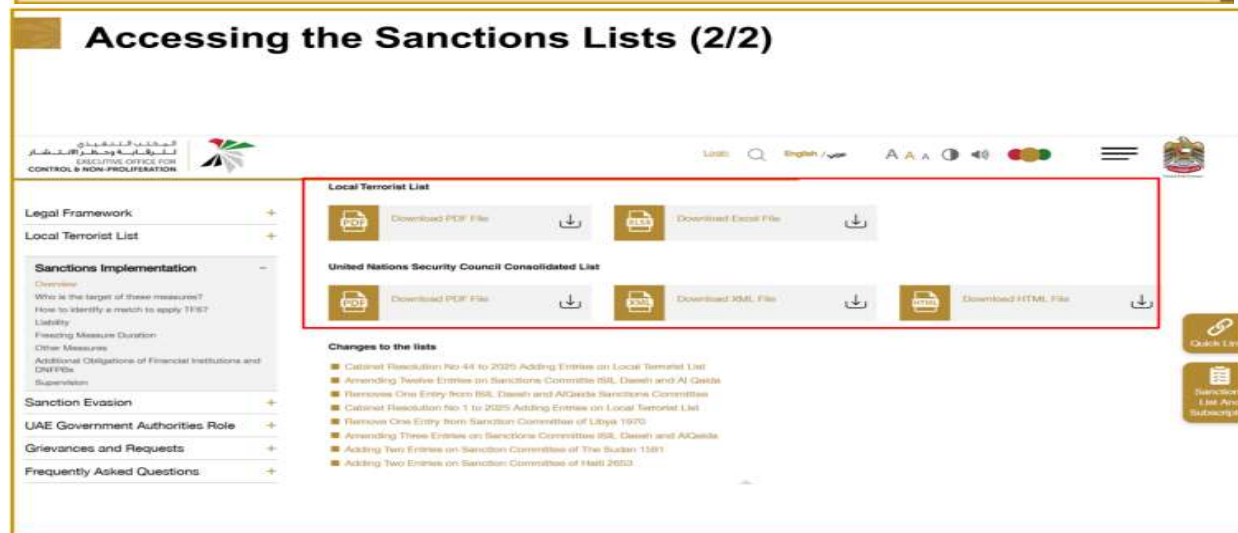
Accessing the Sanctions Lists (1/2)

The Sanctions Lists can be accessed through the EOCN's website



The screenshot shows the EOCN website homepage. The header includes the EOCN logo and navigation links. The main content area is divided into several sections: EOCN, Legislation, Online Services, UAE Control List, Media Center, and Partners. The 'Targeted Financial Sanctions' section is highlighted, and the 'Sanctions Implementation' link is circled in red.

Accessing the Sanctions Lists (2/2)



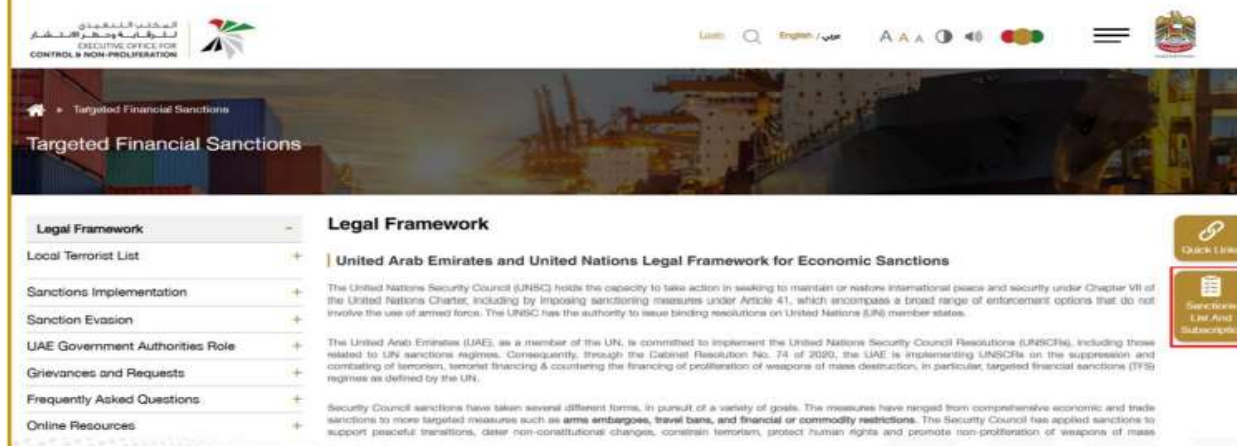
The screenshot shows the 'Sanctions Implementation' page on the EOCN website. The page is divided into two main sections: 'Local Terrorist List' and 'United Nations Security Council Consolidated List'. The 'Local Terrorist List' section has a red box around the 'Download PDF File' and 'Download Excel File' links. The 'United Nations Security Council Consolidated List' section has a red box around the 'Download PDF File', 'Download XML File', and 'Download HTML File' links. Below these sections, there is a 'Changes to the lists' section with a list of updates.

Subscribing to NAS

Subscribe to NAS to receive the latest updates on the Sanctions Lists:

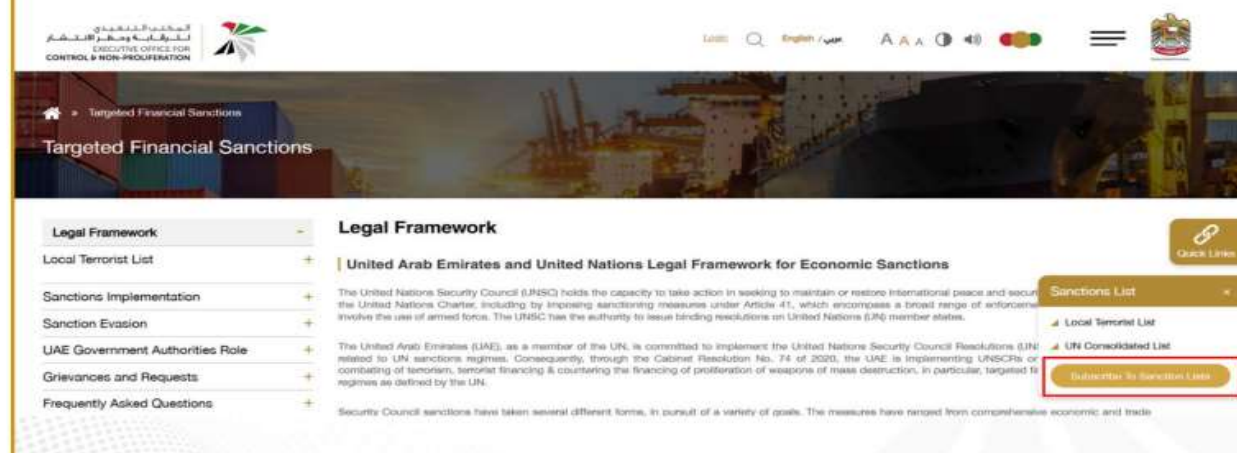
- ❑ Step 1: Access the Targeted Financial Sanctions webpage in the EOCN's website through the following link: <https://www.uaieic.gov.ae/en-us/un-page?p=0#>
- ❑ Step 2: Click on the "Sanctions List And Subscription" icon on the right of the page, followed by "Subscribe to Sanction Lists".
- ❑ Step 3: Fill out your details and click subscribe.
- ❑ Step 4: A pop-up message will appear confirming your subscription.
- ❑ Step 5: You will receive a confirmation email on the registered email address.

Subscribing to NAS (1/5)



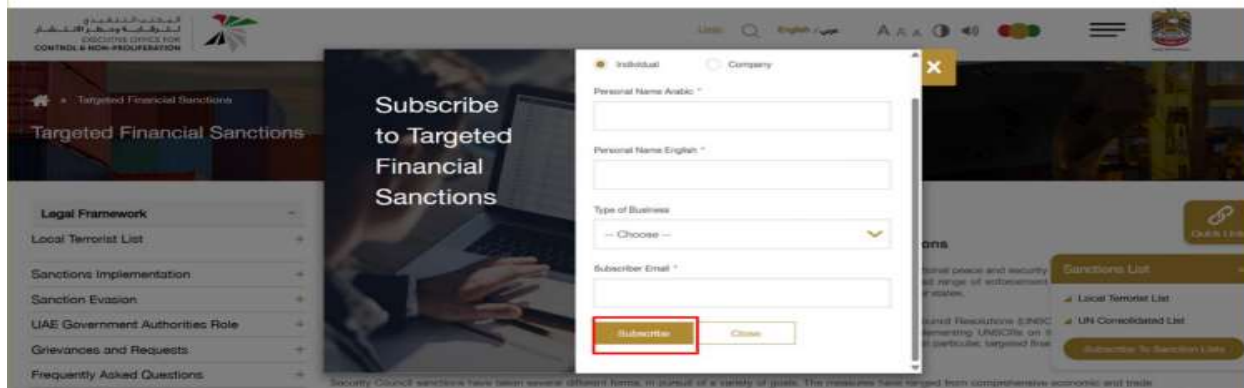
The screenshot shows the 'Targeted Financial Sanctions' webpage. On the left is a sidebar menu with items: Legal Framework, Local Terrorist List, Sanctions Implementation, Sanction Evasion, UAE Government Authorities Role, Grievances and Requests, Frequently Asked Questions, and Online Resources. The main content area is titled 'Legal Framework' and contains the text: 'United Arab Emirates and United Nations Legal Framework for Economic Sanctions'. It explains that the UN Security Council (UNSC) has the authority to issue binding resolutions on UN member states and that the UAE is implementing UNSCRs. A 'Quick Links' box on the right contains a link to 'Sanctions List And Subscription'.

Subscribing to NAS (2/5)



This screenshot shows the same webpage as the previous one, but with the 'Sanctions List' dropdown menu open. The dropdown menu shows two options: 'Local Terrorist List' and 'UN Consolidated List'. Below these options is a red-bordered button labeled 'Subscribe to Sanction Lists'.

Subscribing to NAS (3/5)

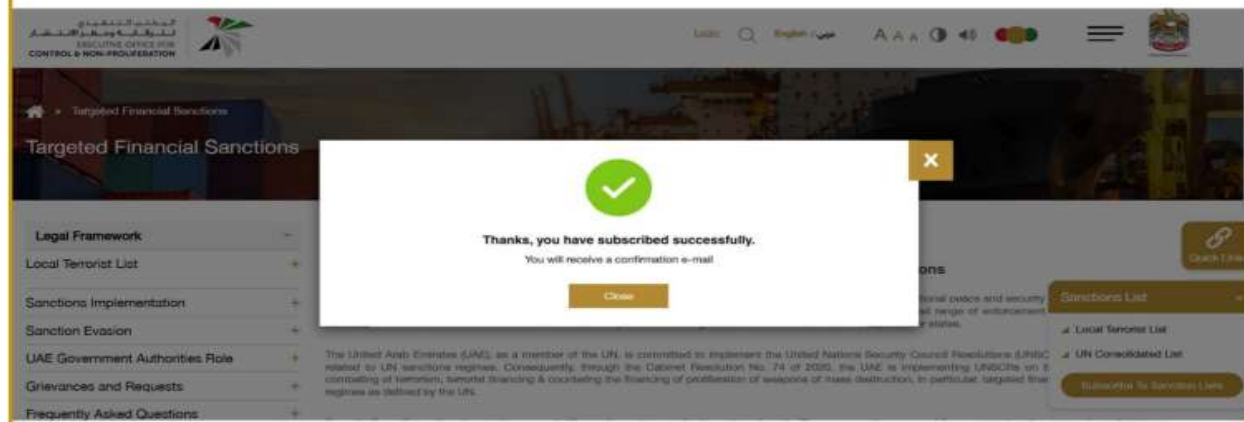


The screenshot shows a web form titled "Subscribe to Targeted Financial Sanctions". The form is for an individual and includes the following fields:

- Personal Name Arabic *
- Personal Name English *
- Type of Business (dropdown menu with "Choose" selected)
- Subscriber Email *

There are "Subscribe" and "Close" buttons at the bottom of the form. The background of the page shows a sidebar with a "Legal Framework" menu and a "Sanctions List" section.

Subscribing to NAS (4/5)



The screenshot shows a confirmation message box with a green checkmark icon. The text inside the box reads:

Thanks, you have subscribed successfully.
You will receive a confirmation e-mail.

There is a "Close" button at the bottom of the message box. The background of the page shows the same sidebar and "Sanctions List" section as in the previous screenshot.

Subscribing to NAS (5/5)

المكتب التنفيذي للرقابة وحظر الانتشار
EXECUTIVE OFFICE FOR CONTROL & NON-PROLIFERATION

الاشتراك في رويات العقوبات المالية المستهدفة

خبري المفضلين

لقد تم التسجيل بنجاح. سيتمكن النظام من إرسال رسائل البريد الإلكتروني الخاصة بالتحديثات لك كلما تم تحديث القائمة.

إذا كنت لا ترغب في تلقي رسائل البريد الإلكتروني فإليك الرابط tf@ecocn.gov.ae لإلغاء الاشتراك.

مع التحية

Subscription To Targeted Financial Sanctions

Dear User

You have successfully subscribed to the Targeted Financial Sanctions list. You will receive the updates whenever a change is applied to the list.

If you don't wish to receive these emails Please contact: tf@ecocn.gov.ae to unsubscribe.

Regards

Government.ae

Alert Update

المكتب التنفيذي للرقابة وحظر الانتشار
EXECUTIVE OFFICE FOR CONTROL & NON-PROLIFERATION

إضافة اسم على قائمة لجنة جزاءات داعش والقاعدة

عزيزي محمد

لنحرص التحديث على قائمة العقوبات ، يرجى [الضغط هنا](#)

وفقاً لقرار مجلس الوزراء رقم 74 لسنة 2020 ، يجب على جميع الأشخاص تطبيق العقوبات المالية المستهدفة والإبلاغ عن نتائج المسح والتحقق والتدابير المتخذة من خلال اتباع إجراءات تطبيق العقوبات المالية المستهدفة الموضحة أدناه:

اتبع إجراءات تطبيق العقوبات المالية المستهدفة

للمسؤول على تفصيل حول تطبيق "العقوبات المالية المستهدفة" ، يرجى [تحميل نسخة من الدليل الإرشادي](#).

تحياتكم

Adding One Entry from ISIL Daesh and AlQaida Sanctions Committee

Dear Mohammad

For details of the sanctions list updates please [click here](#).

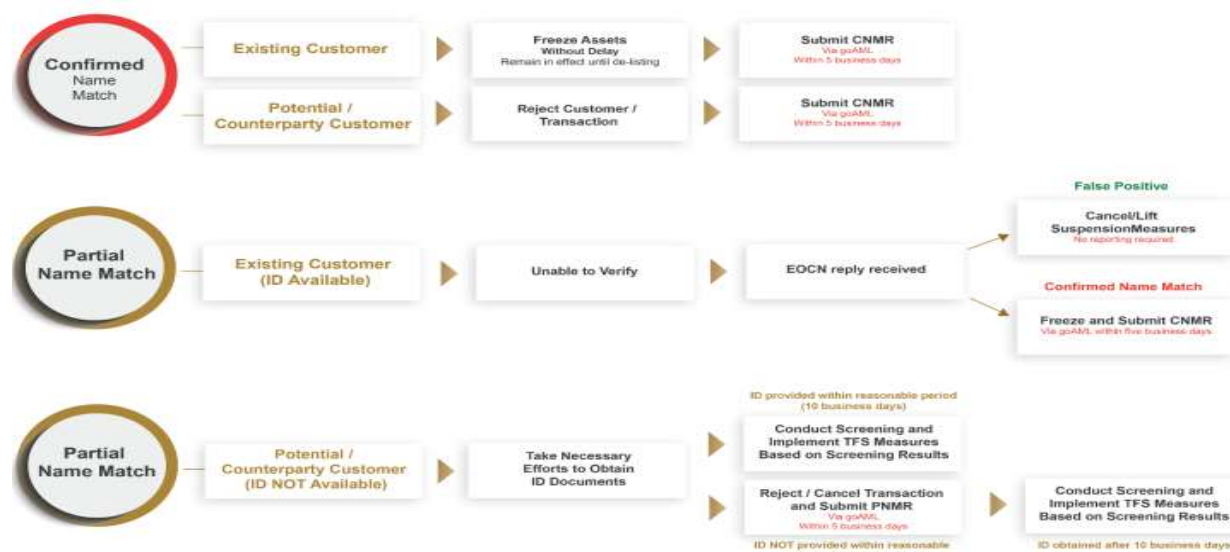
As per [Cabinet Decision 74 of 2020](#), all Persons should implement Targeted Financial Sanctions (TFS) and report all findings and measures taken by following the TFS instructions below:

[Follow TFS Instructions](#)

For details on Target Financial Sanctions implementation, please [download](#) copy of the guideline.

Best regards.

ANNEXURE II TFS REPORTING FLOW CHARTS



ANNEXURE III: FREQUENTLY ASKED QUESTIONS

LEGISLATION

1. What does 'Targeted Financial Sanctions' ("TFS") mean?

The term targeted sanctions means that such sanctions are imposed against specific individuals, entities, or groups (those designated in the Sanctions Lists). 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 group.

2. 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, travelers' 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.

3. 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, Cabinet Decision No. 74 of 2020 established the framework regarding TFS implementation in the UAE, including implementation of TFS on designated Persons in the UAE Local Terrorist List and UNSC Consolidated List.

4. Who must comply with implementing TFS measures?

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.

5. Is my Supervisory Authority going to check compliance with the Cabinet Decision No. 74 of 2020?

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 during their supervisory activities. Non-compliance may result in the application of administrative penalties as well as criminal sanctions as stipulated in the Cabinet Decision. 6. What are the consequences in case of a failure to comply with the obligations set out in Cabinet Decision No. 74 of 2020? 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. 7. Can I be held liable for freezing funds of a designated Persons based on the Cabinet Decision? Any Person who, in good faith, freezes funds or other assets, or refuses to provide financial services to designated individuals, entities, or groups 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.

6. What are the consequences in case of a failure to comply with the obligations set out in Cabinet Decision No. 74 of 2020?

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.

7. Can I be held liable for freezing funds of a designated Persons based on the Cabinet Decision?

Any Person who, in good faith, freezes funds or other assets, or refuses to provide financial services to designated individuals, entities, or groups 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.

FREEZING MEASURES

8. 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). In case the Reporting Entity has come across a ‘Confirmed Name Match’, the term ‘freezing’ is used and the Reporting Entity should apply freezing measures, and it must remain in place until the designated individual, entity, or group is de-listed from the Sanctions Lists or upon a freezing cancellation instruction received from the EOCN.

In case the Reporting Entity has come across a ‘Partial Name Match’ and, after obtaining the ID documentation, is still unsure whether the individual, entity, or group is certainly designated, then the term ‘suspending’ is used and the Reporting Entity should suspend the transaction. Suspension measures should remain in place until further instructions are received from the EOCN on the result of the Partial Name Match (either Confirmed Name Match or False Positive).

9. When should a transaction be rejected or cancelled?

If a Confirmed Name Match is identified on a potential customer (prospective client) or counterparty, then the Reporting Entity is required to reject the business relationship / transaction and report a CNMR within five business days from rejecting the transaction. Similarly, in case a Partial Name Match is identified, and the Reporting Entity is unable to obtain an ID document within a reasonable time period (10 business days) to discount or confirm the match, then the Reporting Entity should reject (cancel) the transaction and report a PNMR within five business days from rejecting the transaction.

10. What does ‘without delay’ mean?

‘Without delay’ means applying freezing measures immediately or in any case within 24 hours upon designation of an individual, entity, or group on the UAE Local Terrorist List or UNSC Consolidated List.

11. How long do I have to keep funds frozen / suspended?

Freezing applied as a result of TFS measures have no time limits. Asset freezes remain valid until one of the following occurs:

- a. The designated Person is delisted (removed) from the Sanctions Lists. Upon delisting, all TFS measures are to be lifted immediately without prior approval from EOCN or the relevant SA, unless there is an active Freeze Order related to the delisted Person issued by a Competent Authority (FIU, Public Prosecution, etc.)
- b. A freezing cancellation decision by EOCN is communicated to the Reporting Entity through goAML.

In case of a Partial Name Match in which the Reporting Entity is unable to verify the match after receiving and reviewing the ID documents and suspension measures were taken, the suspension measures remain until a response is received from the EOCN on the results of the Partial Name Match (either Confirmed Name Match or False Positive).

12. 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 procedures as reflected on the EOCN’s website. The EOCN has also launched an online platform to receive grievance requests and a User Guide on how to submit a request.

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

No. Reporting Entities 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, Reporting Entities must not inform their customers prior to taking the freezing measures.

14. Can permission be obtained to access frozen Funds or Other Assets by the designated individual or entity?

The EOCN, in certain circumstances, may permit access to frozen funds or other assets based on a grievance request received from the designated Person or his legal representative. Please see the Guidance on Grievance Procedures for more information.

SCREENING

15. Can I rely on external service providers to conduct the screening on my behalf?

Reporting Entities may rely on external / third party service providers to conduct screening services on their behalf. However, it is important to note that while such online services are useful, they should not be viewed as an absolute guarantee of compliance with the obligations under the Cabinet Decision and that the ultimate obligation on ensuring compliance with TFS obligations lies with the Reporting Entity. As such, Reporting Entities are advised to do their own checks on the robustness of the screening processes implemented by third party service providers when deciding to utilize their services.

16. Can I use a manual screening process?

Reporting Entities may use a manual screening process, depending on the size and nature of their business. However, the Reporting Entity should take into consideration factors such as the number of clients, the frequency of transactions, and size of the business when deciding on the appropriate screening process (automated v manual). In any case, the Reporting Entity should ensure that adequate screening measures are set in place to identify and implement TFS measures without delay.

17. Should I conduct screening during weekends and public holidays?

In cases of weekends and public holidays, Reporting Entities should have appropriate internal procedures to effectively screen against the UAE Local List and the UNSC Consolidated List and prevent access or use of funds or other assets that may be subject to freezing measures. If the Reporting Entity is not conducting any business activities or transactions and where

customers do not have access to any assets or accounts during weekends or holidays, then the screening obligation starts from the first minute of commencement of business and freezing measures must be applied immediately. In any case, Reporting Entities should ensure that funds or other assets subject to TFS measures are prevented from being accessed or used.

REPORTING

18. What if my existing customer's name partially matches the name of the designated Person, and I am unable to verify whether it is a Confirmed Match or False Positive?

In case a Partial Name Match is identified on an existing customer, it is assumed that the Reporting Entity already possesses the identification documents of the customer and, after reviewing the ID documents, is unable to conclude whether the match is a Confirmed Name Match or False Positive. In this case, the Reporting Entity must suspend without delay any transaction, refrain from offering any funds, other assets or services, and submit a PNMR through GoAML within five business days from implementing suspension measures. The Reporting Entity must ensure that all necessary information and documents regarding the Partial Name Match are submitted and maintain suspension measures until further instructions are received from EOCN via GoAML on whether to cancel the suspension ('False Positive') or implement freezing measures ('Confirmed Name Match').

19. What if a potential customer or counterparty's name partially matches the name of the designated Person, and I am not in possession or unable to obtain the ID documents of the Partial Name Match?

In such cases, the Reporting Entity must first make necessary efforts to obtain identification documents of the potential customer or counterparty to conclude whether the match is a Confirmed Name Match or False Positive. If, after obtaining the ID documents, the Reporting Entity is able to conclude the result as a False Positive, then it may establish the business relation or allow the transaction to proceed without the need to report a PNMR; however, internal documentation of the False Positive result should be maintained.

If the Reporting Entity is unable to obtain the identification documents within a reasonable time (10 business days) of identifying the Partial Name Match, then the transaction or service should be rejected (cancelled) and a PNMR submitted through GoAML within five business days from rejection of the transaction or service, specifying that the transaction has been rejected due to lack of ID documents of the Partial Name Match.

20. Should I report a False Positive Result?

Reporting Entities are not required to report a False Positive result and may allow the business transaction to proceed without notifying the EOCN; however, internal documentation of the screening alert and actions taken need to be maintained.

21. Should I report previous transactions or business dealings with Confirmed or Partial Name Matches?

CNMRs should also be reported on previous business relationships and transactions occurring and accounts held prior to the designation, covering a timeframe of five years. CNMRs should be submitted even if no current funds or other assets are held by the Reporting Entity and includes accounts closed. In this case, the Reporting Entity is required to clarify in the description of the CNMR that no funds or other assets are currently being held, and there is no current business relationship with the Confirmed Name Match, and the status of the account (closed). The same procedure applies to PNMRs.

22. If I identify that a customer is subject to unilateral or multilateral sanctions, however, the customer is not listed on the UAE Local Terrorist List nor the UNSC Consolidated List. Should I report it by raising an CNMR or PNMR?

In case any Confirmed or Partial Name Match is identified to a unilateral / multilateral sanctions list or other criminal lists (i.e. OFAC, EU, HMT, INTERPOL, etc.), the Reporting Entity should not use the CNMR/PNMR reports in GoAml to report such cases, since CNMRs/PNMRs are used to report matches with the UAE Local Terrorist List and UN List only; however, you should consult with your relevant SA on the appropriate course of action and may consider raising an STR/SAR with the FIU in case a match is identified with other sanctions or criminal lists.

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

Any Person (natural or legal) licensed/registered by a SA 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 (CNMRs/PNMRs) to the EOCN and the relevant SA.

FIs, DNFBPs and VASPs that are not registered on GoAML face the risk of being subject to administrative and/or financial sanctions by the relevant SA for failure to register on GoAML. Please contact your relevant SA and the UAE FIU for instructions on how to register.

24. How should I report a Confirmed or Partial Name Match if I am not a GoAML user?

If you identify a Confirmed or Partial Name 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 EOCN on tfs@eocn.gov.ae with details of the case and attaching all supporting documentation.

NOTIFICATION ALERT SYSTEM

25. How can I subscribe to the EOCN Notification Alert System?

To subscribe to the EOCN Notification Alert System, kindly visit the Targeted Financial Sanctions webpage and click on the “Sanctions List and Subscription” icon at the right side of the page to complete your subscription. Please see Annex I: EOCN Notification Alert System Subscription Guide for more details.

26. What steps should I take if I encounter an error when subscribing?

Try to register again, ensuring that you remove any numbers, dashes, brackets, commas, or symbols from the entity name in both Arabic and English. If you continue to receive a rejection, kindly contact us at tfs@eocn.gov.ae.

27. How can I unsubscribe from the Notification Alert System?

Please contact tfs@eocn.gov.ae and state the following information:

- a. Entity name
- b. Entity subscribed e-mail
- c. Reason for unsubscribing

UAE LOCAL TERRORIST LIST AND UNSC CONSOLIDATED LIST

28. Which Sanctions Lists are covered under Cabinet Decision No. 74 of 2020 in terms of the requirement to implement TFS?

The scope of Cabinet Decision No. 74 of 2020 in implementing TFS covers the UAE Local Terrorist List and UNSC Consolidated List only. Other unilateral and multilateral sanctions lists are out of the scope of the Cabinet Decision.

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

You can find out the designated individuals, entities, or groups by checking the updated UAE Local Terrorist List and UNSC Consolidated List in the EOCN website at the links below:

- Local Terrorist List: the link to the UAE Local Terrorist List can be found at the bottom of the Sanctions Implementation webpage on the EOCN website (scroll to the bottom of the page) and is available in both PDF and Excel format. ()
- UNSC Consolidated List: The UNSC publishes a list of all the sanctioned individuals, entities, or groups designated by the United Nations Sanctions Committees or directly by the UNSC. ()