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

VERSION: FALCON PRECIOUS METAL REFINERY (FZC) /V3

Title	**Targeted Financial Sanctions Related to Terrorism, Terrorism Financing and Proliferation Training Policy**
Information Classification	**Internal**
Policy Supported	**FALCON PRECIOUS METAL REFINERY (FZC)**
Current Version	**V.3**
Review Cycle	**Annually**
Effective Date	**May 2025**
Due Date for Review	**April 2026**

Document Contact details

Role	Designation
Reviewed By	**Senior Management**
Approved	**Owner**

Document Revision History:

Revision No	Effective Date	Revision History	Due Date
V.1	**May 2023**	**Initial Creation**	**April 2024**
V.2	**May 2024**	**Reviewed and Updated**	**April 2025**
V.3	**May 2025**	**Reviewed and Updated**	**April 2026**

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.

Document Title	FALCON PRECIOUS METAL REFINERY (FZC)	Signature
Prepared By	Compliance officer	
Reviewed By	Manager	
Approved By	Owner	

SAIF ZONE Sharjah - U.A.E. FALCON PRECIOUS METAL REFINERY (FZC)

COMPANY PROFILE

Legal Name as per Trade License	:	**FALCON PRECIOUS METAL REFINERY (FZC)**
Legal Type	:	Free Zone Co. with Limited Liability
DNFBP Category	:	Dealers in Precious Metals and Stones
Licensing Authority	:	Sharjah Airport International Freezone
License Number	:	22817
Incorporation Date	:	9th December 2021
Principal Activities	:	Gold Refinery
Authorized Person Name	:	Satish Bansal
MLRO / Compliance Officer	:	Manish Rawat
Office Address	:	600 M2 Warehouse T5-020, Sharjah, UAE
Mobile Number	:	+971 54-279 0394
Phone Number	:	+971 6 575 5324
Email id	:	admin@falconrefinery.com

Details of Beneficial Owner

Sl. No.	Name	Nationality	ID Number	Shareholding %
1	Vinod Puranmal Bansal	INDIA	784-1953-5576785-6	90 %
2	Satish Bansal Puran Mal Bansal	INDIA	784-1957-7105097-8	10 %

Table of Contents

Abbreviations of Common Terms

Terms	Definitions
AML & CFT	Anti-Money Laundering. all references in this document to AML will include obligations for Countering the Financing of Terrorism (CFT), Countering Proliferation Financing (CPF) and Other Identified Risks unless the context requires otherwise. The financing of terrorism involves the raising and processing of funds, from both legal and illegal sources, to supply terrorists with resources to carry out their attacks. While the phenomena differ in keyways, they often seek to exploit the same vulnerabilities that allow for an inappropriate level of anonymity and non-transparency in the execution of transactions.
FIU	Financial Intelligence Unit means the agency will collect raw transactional information and Suspicious activity reports (SAR) usually provided by banks and other entities as part of regulatory requirements.
DNFBPs	Designated Non-Financial Businesses and Professions (DNFBPs) Means Real estate agent & Dealers in precious metals. Dealers in precious stones. Lawyers, notaries, other independent legal professionals and accountants.
OECD Guidance	Organization for Economic Co-operation and Development Means the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas;
Beneficial Owner	Beneficial Owner is defined in Article (5) of the Cabinet Decision No. (58) of 2020 Regulating the beneficial Owner Procedures: 1. "The Beneficial Owner of the Legal Person shall be whoever person that ultimately owns or controls, whether directly through a chain of ownership or control or by other means of control such as the right to appoint or dismiss the majority of its Directors, 25% or more of the shares or 25% or more of the voting rights in the Legal Person." 2. The Beneficial Owner may be traced through any number of Legal Persons or arrangements of whatsoever kind. 3. If two or more natural persons jointly own or control a ratio of capital in the Legal Person, all of them shall be deemed as jointly owners or controllers of such ratio. 4. If, after all reasonable means have been taken, no natural person is identified as an ultimate Beneficial Owner in accordance with Clause (1) of this Article, or there is reasonable doubt that any natural person identified as an ultimate Beneficial Owner is the true Beneficial Owner in the Legal Person; then the natural person who controls the Legal Person by other means of control shall be deemed as the Beneficial Owner. 5. Where no natural person is identified in accordance with Clause (4) of this Article; then the natural person who holds the position of a higher management official shall be deemed as the Beneficial Owner
Business relationship	means a business, professional or commercial relationship between the client and the obliged entity which is connected with the professional activities of an obliged entity, and which is expected by the obliged entity, at the time when the contact is established, to have an element of duration

Client / Customer	**A Client (identical meaning to Customer) should be understood as natural person or a legal person / entity with which the reporting entity has a business relationship or for whom the reporting entity carried out an occasional transaction. In this context, customers refer to all existing customers with whom the entity has had a business relationship within the reporting period including occasional (walk in) customers who have been serviced during the reporting period. Reference to customers is made in respect of those that were provided with a relevant activity or relevant service that falls under AML/CFT regulations by the reporting entity. For more information, please see Cabinet Decision No. (10) Of 2019 concerning the implementing Regulation of Decree Law No. (20) Of 2018, Article 1 (definition of a "Customer), Article 2 and 3 (activities and transactions that fall under the scope of the AML/CFT regulations).**
Governance	**Governance related requirements are stipulated under AML/CFT Law No.20 of 2018, Article 16.1(d) and AML/CFT Cabinet Decision No. (10) of 2019, Article 4.2(a), 20, 21, 2 Term Definition 44.4 and AML/CFT guidance for Designated Nonfinancial Businesses and Professions (DNFBPs) issued by the Ministry of Economy (April 1, 2019), Article 8.**
LLC	**LLC - Limited Liability Company; For definitions of different types of establishments please refer to Federal Law No 2 of 2015 on Commercial Companies**
Controlling Shareholder	**A shareholder who has the ability to directly or indirectly influence or control the appointment of the majority of the board of directors, or the decisions made by the board or by the general assembly of the entity, through the ownership of a percentage of the shares or stocks or under an agreement or other arrangement providing for such influence.**
Direct Relationship	**A relationship between two parties that knowingly provide the other material, technological, logistical, or financial support and both parties are directly impacted by the other party.**
Indirect Relationship	**A relationship between two parties that affect each other through a third-party source or one or more intermediaries.**
Listed Person	**Individuals, legal entities and groups listed by the UN Security Council on the UN Consolidated List or listed by the UAE Cabinet on the Local Terrorist List, as the case may be.**
Listing	**Identifying the individuals, legal entities and groups subject to sanctions imposed pursuant to relevant UNSC Resolutions ("UNSCRs"), decisions of the Sanctions Committee, or relevant decisions of the UAE Cabinet, as the case may be, and implementing relevant sanctions against such individuals, legal entities and groups, with a statement of the reasons for Listing.**
Local Terrorist List	**Terrorism lists issued by the UAE Cabinet pursuant to the provisions of Article (63) paragraph (1) of Federal Law No. (7) of 2014 on Combating Terrorism Offences**
Other Measures	**Sanction measures other than freezing that must be enforced, and which may be included in Relevant UNSCRs or UAE Cabinet decisions regarding the issuance of Local Terrorist List, such as prohibitions relating to travel, weapons, imports, or provision of fuel supplies and other.**

Previous Customer	**A customer with whom the relationship was terminated and the LFI maintains relevant records according to record keeping and other requirements.**
Relevant UNSCRs	**All current and future UNSCRs relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, including but not limited to Resolutions 1267 (1999), 1373 (2001), 1988 (2011), 1989 (2011), 1718 (2006), 2231 (2015) and any successor resolutions.**
Sanctions Committee	**Any of the UN Security Council Committees established as per its resolutions, including UNSCRs 1267 (1999) and 1989 (2011) relating to ISIL and Al-Qaida, 1988 (2011) relating to the Security and Stability of Afghanistan, and 1718 (2006) relating to the suppression and combating of proliferation of weapons of mass destruction for the DPRK.**
Subsidiary	**An entity owned by another entity by more than 50% of its capital or under full control of that entity regarding appointment of the Board of Directors.**
Targeted Financial Sanctions (TFS)	**The term Targeted Financial Sanctions means that such sanctions are against certain individuals, entities, groups, or undertakings. The term Targeted Financial Sanctions includes both asset freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned.**
The Executive Office	**The Executive Office of the Committee for Goods and Materials Subject to Import and Export Control.**
UN Consolidated List	**A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and it's financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their Listing.**
Without Delay	**Within 24 hours of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.**
Proliferation	**Proliferation is the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. Includes technology, goods, software, services or expertise.**
Proliferation Financing	**Proliferation is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.**

"PEPs"	**"Politically exposed persons" When individuals are elected to prominent political positions or assigned high-profile public roles, they should be categorized as politically exposed persons (PEPs) to reflect their increased risk of involvement in money laundering or terrorism financing.**
DPEP	**The FATF Guidance for PEPs also defines Domestic PEPs as high-risk individuals located in the same country as the financial institution of which it is a client and has a domestically located position. These domestic high-risk individuals are defined as officials of a local political party, senior politicians, heads of state companies, or senior military officials.**
FPEP	**"Foreign Politically exposed persons" Means persons holding an important public position on behalf of a government that differs from the government's public position in which the financial institution is located.**
TFS	**Targeted Financial Sanctions are measures for asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of specified entities/ designated persons who are being sanctioned.**
APG	**The Asia/Pacific Group on Money Laundering is an inter-governmental organization, consisting of 41 member jurisdictions. The objective of the APG is to ensure that individual members effectively implement the international standards against money laundering, terrorist financing and proliferation financing related to weapons of mass destruction.**
FATF. "Financial Action Task Force"	**The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard**
EAG "Eurasian group on "	**The Eurasian group on combating money laundering and financing of terrorism (EAG) is a FATF-style regional body which comprises 9 countries: Belarus, China, Kazakhstan, Kyrgyzstan, India, Russia, Tajikistan, Turkmenistan and Uzbekistan. EAG is an associate member of the FATF.**
HSI	**Homeland Security Investigations (United States) is the principal investigative arm of the U.S. Department of Homeland Security, responsible for investigating transnational crime and threats, specifically those criminal organizations that exploit the global infrastructure through which international trade, travel and finance move.**
Jewellers	**"Jewellers" means a person who is a bullion dealer or engaged in sale of jewelry, precious stones and metals including all articles made wholly or mainly of gold, platinum, diamonds of all kinds, precious or semi-precious stones, pearls whether or not mounted, set or strung and articles set or mounted with diamonds, precious or semiprecious stones or pearls.**
Recycled Gold and/or Precious Metals	**Means gold and/or precious metals that has been previously refined, such as end-user, post-consumer and investment gold and/or precious metals and gold and/or precious metals-bearing products, and scrap and waste metals and materials arising during refining and product manufacturing including recovered material from industrial recovery, which is returned to a refiner or another downstream intermediate processor to begin a new life cycle as**

	'recycled gold'. The origin of Recycled Gold and/or Precious Metals is considered to be the point in the supply chain where the gold and/or precious metals is returned to the refiner or other downstream intermediate processor or recycler; assay samples are excluded from this category and falls out of scope of the review provided the member is able
Gold Bullion	**Bullion means precious metal bars and coins (gold, silver, and platinum) that are designated for trading through their sale or purchase in units of ounces, kilograms and/or ten tolas and are considered high quality precious metals, unless stated otherwise by the company, and comply to the minimum purity requirements of the Dubai Good Delivery (DGD) and London Good Delivery (LGD) standards.**
Gold Ingot	**A gold bar, also called gold bullion or gold ingot, is a quantity of refined metallic gold of any shape that is made by a bar producer meeting standard conditions of manufacture, labeling, and record keeping. Larger gold bars that are produced by pouring the molten metal into molds are called ingots.**
ASM	**Artisanal and small-scale mining (ASM) is largely an informal sector with limited available information on production, revenues, operations and even location of activities. Regulation of the sector is often inadequate and its real contribution to a national economy is difficult to estimate.**
LSM	**Large-scale or medium-scale mining is governed by a framework of regulatory controls, permits and inspections and is subject to health, safety, social, environmental, closure and governance standards. Large-scale mining involves the payment of royalties and other taxes to governments in return for developing publicly owned mineral resources.**
CDD	**"Customer due diligence" Means that part of the KYC process where information that comprises facts about a client is gathered by the dealer to assess the extent to which the client exposes the dealer to arrange of risks.**
Transaction	**Transaction is defined under Article 1 of the Cabinet Decision No. (10) Of 2019 "Transaction: All disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation." For the purpose of this questionnaire, transaction and payment should have an identical meaning.**
Occasional Transaction	**Any Transaction other than a Transaction carried out in the course of an established Business Relationship.**
Suspicious transaction report	**A suspicious transaction is a transaction that causes a reporting entity to have a feeling of apprehension or mistrust about the transaction considering its unusual nature or circumstances, or the person or group of persons involved in the transaction.**

1. Introduction

We value the importance of having documented Targeted Financial Sanctions (TFS) policies and procedures and are committed to adhering to regulatory requirements. This proactive approach not only helps protect our business but also demonstrates a strong commitment to compliance and ethical business practices.

By implementing and following these policies, we can ensure that our dealings with customers and clients are in full compliance with sanctions regulations, thereby minimizing the risk of inadvertently engaging in transactions with sanctioned entities.

Our dedication to ensuring that our clients are free from any sanctions highlights our commitment to maintaining a transparent and trustworthy business environment. This approach not only safeguards our business reputation but also builds trust with our clients and partners.

As a retail and wholesale distribution network, we likely engage in cross-border transactions and deal with diverse entities. Having documented TFS policies allows us to conduct enhanced due diligence on potential partners, suppliers and customers, providing an additional layer of protection for our business.

It's evident that we understand the significance of compliance and the potential consequences of non-compliance with TFS regulations. By being diligent in this aspect, we can continue to provide excellent service to our customers while ensuring that our business remains on the right side of the law.

The term Targeted Financial Sanctions means both 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 (Source: FATF Glossary).

The United Nations Security Council Sanctions Regimes defines ‘Targeted’ as: ◦ meaning that they are intended to have limited, strategic focus on certain individuals, entities, groups or undertakings. The most common sanctions measures are travel bans, asset freezes and arms embargoes.

The purpose of this policy is to assist our sector in establishing strong systems and in becoming partners in the fight against Targeted Financial Sanctions. Its objective is also to help our company in understanding its Targeted Financial Sanctions Related to Terrorism, Terrorism Financing and Proliferation Training obligations.

1.2 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.

1.3 Objectives of Financial Sanctions

Financial Sanctions are imposed to:

i. 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,

ii. Constrain a target by denying them access to key resources needed to continue their offending behavior, including the financing of terrorism or nuclear proliferation.

iii. Signal disapproval, stigmatizing and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or

iv. 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.

1.4 Policy Compliance and Custodian

The purpose of this policy (the "Policy") is to set out the responsibilities of FALCON PRECIOUS METAL REFINERY (FZC) 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, FALCON PRECIOUS METAL REFINERY (FZC) 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) Of 2019, Concerning the Implementing Regulation of Decree-Law No. (20) Of 2018. 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) FALCON PRECIOUS METAL REFINERY (FZC), (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 FALCON PRECIOUS METAL REFINERY (FZC) operates.

1.5 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 FALCON PRECIOUS METAL REFINERY (FZC) policies and procedures and to be alert to any behavior or actions that are inconsistent with FALCON PRECIOUS METAL REFINERY (FZC) 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 FALCON PRECIOUS METAL REFINERY (FZC) shall appoint a compliance officer who will provide expertise and assistance regarding the implementation and enforcement of this Policy thus supporting the Top Management.

2. Overview of the Targeted Financial Sanctions Related to Terrorism, Terrorism Financing and Proliferation Training

2.1 National Legislative and Regulatory Framework

Legislative Compliance means adhering to the requirements of law, industry and organization standards and codes, the principles of good governance, as well as accepted community and ethical standards.

2.2 International Legislative and Regulatory Framework

Regulatory compliance is when businesses follow state, federal and international laws or regulations relevant to operations Obligations. References to 'legislative compliance obligations' are references to obligations imposed by an Act and all subordinate legislation to that Act (including Regulations, Determinations, Orders, Rules) and relevant mandatory Standards and Codes.

The AML/CFT legislative and regulatory framework of the UAE is part of a larger international AML/CFT legislative and regulatory framework made up of a system of intergovernmental legislative bodies and international and regional regulatory organizations. On the basis of international treaties and conventions in relation to combating money laundering, the financing of terrorism and the prevention and suppression of the proliferation of weapons of mass destruction, intergovernmental legislative bodies create laws at the international level, which participating member countries then transpose into their national counterparts. In parallel, international, and regional regulatory organizations develop policies and recommend, assess and monitor the implementation by participating member countries of international regulatory standards in respect of AML/CFT.

Among the major intergovernmental legislative bodies, and international and regional regulatory organizations, with which the government and the Competent Authorities of the State actively collaborate within the sphere of the international AML/CFT framework are:

- The United Nations (UN)

- The Financial Action Task Force (FATF). The Financial Action Task Force (FATF) is an intergovernmental body established in 1989, which sets international standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. FATF also monitors the implementation of its standards, the 40 'FATF Recommendations', by its members and ensures that the 'FATF Methodology' for assessing compliance with the FATF Recommendations is properly applied by all FSRBs.

- The Middle East and North Africa Financial Action Task Force (MENAFATF). Recognizing the FATF 40 Recommendations on Combating Money Laundering and the Financing of Terrorism and Proliferation, and the related UN Conventions and UN Security Council Resolutions, as the worldwide-accepted international standards in the fight against money laundering and the financing of terrorism and proliferation, MENAFATF was established in 2004 as a FATF Style Regional Body (FSRB), for the purpose of fostering co-operation and co-ordination between the countries of the MENA region in establishing an effective system of compliance with those standards. The UAE is one of the founding members of MENAFATF.

2.3 National AML/CFT Strategy Framework

Money laundering and the financing of terrorism are crimes that threaten the security, stability and integrity of the global economic and financial system, and of society as a whole. The estimated volume of the proceeds of crime, including the financing of terrorism, that are laundered each year is between 2-5% of global GDP. Yet, by some estimates, the volume of criminal proceeds that are actually seized is in the range of only 2% of the total, while roughly only half of that amount eventually ends up being confiscated by competent judicial authorities. Combating money laundering and the financing of terrorist activities is therefore an urgent priority in the global fight against organized crime.

The UAE is deeply committed to combating money laundering and the financing of terrorism and illegal organizations. To this end, the Competent Authorities have established the appropriate legislative, regulatory and institutional frameworks for the prevention, detection and deterrence of financial crimes, including ML/FT. They also continue to work towards reinforcing the capabilities of the resources committed to these efforts, and towards improving their effectiveness by implementing the internationally accepted AML/CFT standards recommended and promoted by FATF, MENAFATF and the other FSRBs, as well as by the United Nations, the World Bank and the International Monetary Fund (IMF).

As part of these efforts, the Competent Authorities of the UAE have taken a number of substantive actions, including among others:

- Enhancing the federal legislative and regulatory framework, embodied by the introduction of the new AML/CFT Law and Cabinet Decision, which incorporate the FATF standards;

- Conducting the National Risk Assessment (NRA) to identify and assess the ML/FT threats and inherent vulnerabilities to which the country is exposed, as well as to assess its capacity in regard to combating ML/FT at the national level;

- Formulating a National AML/CFT Strategy and Action Plan that incorporate the results of the NRA and which are designed to ensure the effective implementation, supervision, and continuous improvement of a national framework for the combating of ML/FT, as well as to provide the necessary strategic and tactical direction to the country's public and private sector institutions in this regard.

- The National Strategy on Anti-Money Laundering and Countering the Financing of Terrorism of the United Arab Emirates is based on four pillars, each of which is associated with its own strategic priorities. These strategic priorities in turn inform and shape the key initiatives of the country's National Action Plan on AML/CFT.

- The pillars of the National AML/CFT Strategy, together with their strategic priorities are summarized in the table below:

National AML/CFT Strategic Pillars	Strategic Priorities
Legislative & Regulatory Measures	Increase effectiveness and efficiency of legislative and regulatory policies and ensure compliance
Transparent Analysis of Intelligence	Leverage the use of financial databases and the development of information analysis systems to enhance the transparent analysis and dissemination of financial intelligence information
Domestic and International Cooperation & Coordination	Promote the efficiency and effectiveness of domestic and international coordination and cooperation with regard to the availability and exchange of information
Compliance and Law Enforcement	Ensure the effective investigation and prosecution of ML/FT crimes and the timely implementation of TFS

The National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations has identified a number of key drivers of success in achieving the goals of the National AML/CFT Strategy. These include, among other things, ensuring:

- Effective coordination between the Financial Intelligence Unit (FIU), Law Enforcement Authorities, Public Prosecutors, Supervisory Authorities, and other Competent Authorities within the country.

- Effective compliance with the laws and regulations governing banking activities and other financial services.

- Awareness by DNFBPs of the relevant ML/FT risks facing the UAE in general and their sectors in particular, as informed by the results of the NRA, as well as their awareness of their statutory obligations in regard to the management and mitigation of those risks.

- The present Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations Guidelines for Designated Non-Financial Businesses and Professions are thus intended to advance the efforts of the Committee, the Supervisory Authorities, and the other Competent Authorities of the State in this direction.

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

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

- This policy is therefore focused on the procedures to implement the UN and local TFS regimes by all Persons (natural and legal) the UAE. Financial Institutions and DNFBPs are obliged, by UAE law, to apply policies, procedures and controls to implement TFS to those sanctioned and referred in the UN List and the Local Terrorism List.

The following list comprises of all of the relevant Laws/Executive Regulations, Guidelines, and Notices issued so far for the purpose of implementing UN Financial Sanctions and local TFS measures in the UAE.

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

3. What are Targeted Financial Sanctions (TFS)?

- 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.

4. What is United Nations Security Council Resolution (UNSCR)?

- 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

5. 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.

- 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.

5.1 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

5.2 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).

5.3 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

5.4 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.

5.5 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.

5.6 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.

5.7 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.

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

a. Terrorism and terrorist financing:

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

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

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

c. Other UN sanctions regimes with TFS:

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

5.8 Describe your 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 Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and illegal Organizations ("AMLCFT Law"), Cabinet Decision No.10 2019 concerning the Implementing Regulation of the AMLCFT Law ("New Sanctions Regulations") 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").

- Others: Where sanctions are issued by inter-governmental organizations ("IGOs") of which the UAE is a member, these sanctions are implemented by adding the sanctioned persons to the Sanctions List (as stated above) and/or issuing internal circulars to the relevant governmental entities.

With respect to trade specifically, the Ministry of Economy is responsible for regulating trade restrictions and sanctions; for instance, it recommended issuance of Federal Law No 13 of 2007 concerning the Commodities subject to the Monitoring of Imports and Exports ("Commodities Law"), which, among others, prohibits the export or re-export of strategic goods and dual-use items without a special license.

In addition to the above methods, multiple laws and regulations are regularly issued to additionally impose restrictions and require that persons in the UAE, particularly in financial and regulated industries, undertake implementation measures such as reporting requirements and clients due diligence, in order to ensure compliance with 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.

5.9 The relevant government agencies that administer or enforce the sanctions regime.

The UAE administers sanctions through different government entities, depending on the implementation measures required for the imposition of the relevant sanctions.

- **Office:** The Commodities Law authorizes the restriction or ban on Import, Export or Re-export of goods demand as a treat to the UAE's foreign policy. As the UAE Authority responsible for implementing the AML/CFT, the office articulates obligations in the New SR Guidance having that force of Law.

- **Customs authorities:** To the extent where they are able and empowered to confiscate and freeze any funds that is in breach of any applicable sanctions in the UAE.

5.10 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.

A. 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. The UAE Cabinet and the UN Security Council impose sanctions by issuing the Local List and Sanctions List, and Local List to the public by publishing the same on its website. It also issued guidance on implementation regulations of the New Sanctions Regulations, which include additional obligations on all UAE persons.

As illustrated sanctions have also in the past been imposed by way of the issuance of Federal Laws and Cabinet Decisions; however, this occurs less often.

The UAE may, in certain circumstances, implement sanctions issued by IGOs (other than the UN) of which it is a member and would update its sanctions list to that effect.

B. Jurisdiction implements United Nations sanctions.

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

The UAE implements UN Sanctions issued by the UN Sanctions Committee. The AML/CFT Law requires "prompt application of the directives when issued by the competent authorities in the state for implementing the decisions by the UNSC under Ch. 7 of UN Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of weapons of mass destruction, and other directives".

The New Sanctions Regulations and New SR Guidance set out the implementation framework of the Sanctions List, including the coordination and implementation role of the Office. The Office imposes direct responsibilities on and accords power to the supervisory authorities of FIs and DNFBPs to implement the Sanctions List. Moreover, the New SR Guidance imposes obligations on FIs and DNFBPs, and all other natural and legal persons in the UAE, to implement the Sanctions List. DNFBPs consist of anyone or more of the commercial or professional activities listed in the implementing regulation of the AMLCFT Law, which include certain real estate brokers and agents, merchants of precious metals and precious stones, lawyers and providers of corporate services.

Pursuant to the New SR Guidance, the office has imposed a number of obligations on all persons in the UAE (legal and natural) including DNFBPs and FIs, to ensure implementation of UN Sanctions.

- All such persons must register with the office, and the Office shall inform them, via automated email notifications, of any changes to the Sanctions List.
- All such persons are required to have screening measures in place which must be undertaken on daily basis as per the requirements in the New SR Guidance.
- Application of targeted financial sanctions ("TFS"), including by freezing funds, and not making funds available.
- Notification requirements.

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 nothing 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 Corporation 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.

C. 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 affected 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.

D. Can the public access those lists?

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

a. With respect to the Local List (https://www.uaeiec.gov.ae/en-us/un-page)
b. 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.

E. 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.

F. 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.

G. The Process for lifting sanctions

The process for listing sanctions varies depending on the method of imposition as well as the nature of such sanction.

With respect to sanctions issued by IGOs, sanctions are added and removed by the relevant IGO. The removal of such sanctions is then implemented by the UAE through different means, which may vary depending on the method by which the relevant sanction was imposed.

H. Jurisdiction has an export control regime that is distinct from sanctions.

Although the export control regime of the UAE is distinct from sanctions, it plays an important role in enforcing sanctions where the same is with respect to the export or import of sanctioned products from sanctioned countries/persons. This is particularly illustrated by the significant role accorded to the Office with respect to implementing the Sanctions List, as well as the Commodities Law, which includes banning the import, export or re-export of goods deemed a threat to the UAE's foreign policy (sanctions are often used as an instrument of foreign policy).

I. Jurisdiction has blocking statues or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes.

The UAE does not have blocking statues or other restrictions prohibiting adherence to other jurisdictions' sanctions or embargoes.

J. Implantation 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 on the nationality of the 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.

K. 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").

1. 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.

2. 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.

L. 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.

M. 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 as 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.

Furthermore, Article 21 of the New Sanctions Regulations and Sections 4(4) and 5 of the Sanctions Implementation Regulations impose several reporting obligations on FIs and DNFBPs to the relevant financial regulator, including in the following case:

- Where it has frozen funds pursuant to issued sanctions.
- Where any of its former customers or an accidental customer dealt with is a person listed on the Sanctions List;

- Where it has decided not to undertake procedures because of the similarity of names which is unable to be resolved using available or accessible information; and
- Where it has unfrozen funds/property pursuant to an unfreezing order.

Also, under Section 5 of the New SR Regulations, all UAE natural and legal persons must inform the "*competent authorizes"* where they have frozen funds in its possession, under its control, or management, belonging to a Designated Person or to a person representing a Designated Person.

N. The government conveys its compliance expectations.

Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme 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.

In financial free zones, compliance expectations are comprehensive and included in "Rulebooks". Furthermore, Article 22 of the New Sanctions Regulations imposes an obligation on financial regulators to take all measures to ensure FIs and DFNBPs comply with sanctions and apply administrative sanctions upon violation of such compliance.

A common compliance policy required is the implementation of client due diligence and onboarding clearances to ensure that the customers of such institutions are not subject to any sanctions.

At a more general level, Section 5 of the New SR Guidance requires all natural and legal persons to (1) without delay or prior notice, freeze funds in its possession, under its control or management, belonging to a Designated Person, controlled over, fully or partially, directly or indirectly, or belonging to a person functioning on behalf of a Designated Person, or under its direction, or owned or controlled over by that Designated Person (directly or indirectly); and (2) inform the "competent authorities" where they have frozen funds in its possession, under its control, or management, belonging to a Designated Person representing a Designated Person.

6 Enforcement

6.1 There are criminal penalties for violating economic sanctions laws and/or regulations.

There are criminal penalties for violating economic sanction laws and/or regulations where such violation also constitutes a crime under Federal Law 3 of 1987 on the issuance of the Penal Code ("Penal Code") or other applicable laws, such as the Anti-Terrorism Law, Commodities Law, and AMLCFT Law. Article 23 of the New Sanctions Regulations provides that any violation thereof is subject to the penal and administrative sanctions set forth under the AMLCFT Law. For example, pursuant to Article 28 of the AMLCFT Law, "imprisonment or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) shall be applied to any person who violates the instruction issued by the competent authority in the UAE for the implementation of the directives of UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction and other related decisions".

6.2 The government authorities are responsible for investigating and prosecuting criminal economic sanctions offences.

The government authorities responsible for investigating criminal economic sanctions offences differ depending on the nature of the sanctions.

As explained above, different government authorities are responsible for implementing different types of sanctions; these very same government authorities must investigate any potential breach by a person under its surveillance.

These governmental authorities must then report to the executive board of the Supreme Council for National Security or the Public Prosecution as applicable, which will further investigate the matter and may file a claim for prosecution of any person found to be in breach of sanctions by way of unauthorized exports/imports.

These governmental authorities must then report to the executive board of the Supreme Council for National Security or the Public Prosecution as applicable, which will further investigate the matter and may file a claim for prosecution of any person found to be in breach of sanctions through the judiciary system.

6.3 There is both corporate and personal criminal liability.

There is both corporate and personal criminal liability. This is expressly sated, among others, under Article 42(3) of the Anti-Terrorism Law and Article 4 of the AMLCFT Law.

The maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations.

Pursuant to Article 42 of the Anti-Terrorism Law, a maximum of AED 100 million shall be imposed upon a judicial person who violates criminal sanctions, unless a more serve penalty is imposed under the Penal Code. Article 162 of the Penal Code provides for a fine of not less than AED 1 million where a person imports/exports to an enemy country in time of war.

Under the Commodities Law, an individual can be fined up to AED 500,000.

6.4 There are other potential consequences from a criminal law perspective.

Other potential consequences for breach of sanctions, where such breach constitutes crimes under the Anti-Terrorism Law or Penal Code, include imprisonment and capital punishment. The Commodities Law also provides for imprisonment for up to one year. Public prosecution may be involved if the issue relates to a crime punishable by law, such as felonies.

The AMLCFT Law lists potential consequences for breaches thereof, including:

Banning the violator from working in the sector related to the violation for the period determined by the supervisory authority.

Constraining the powers of the board members, supervisory or executive management members, managers or owners who are proven to be responsible for the violation;

Arresting managers, board members and supervisory and executive management members who are proven to be responsible for the violation for a period to be determined by the supervisory authority or requesting their removal; and cancelling the license of the violator.

There are civil penalties for violating economic sanctions laws and/or regulations.

There are civil penalties for violating economics sanctions, laws and regulations. These penalties depend on the nature of the violation in question. Persons violating custom laws may find themselves fined or their assets seized and/or destroyed.

6.5 The government authorities are responsible for investigating and enforcing civil economic sanctions offences.

The government authority responsible for investigating and enforcing civil economic sanctions would normally be the supervisory authority of the entity/person involved in such breach, but also depends on the nature of the sanction that was breached.

6.6 There is both corporate and personal civil liability.

There is both corporate and personal liability for civil economic sanctions violations. The laws and procedures applicable where civil economic sanctions are violated include the blocking of transactions and imposition of administrative fines by the competent authorities.
There are maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions.

6.7 The maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions

Administrative penalties may apply where persons are found to have violated economic sanctions; the penalty amount differs depending on the severity of the violation. With respect to customs offences, persons may be fined varying amounts depending on the offence and the value of the related goods.

For instance, under Article 28 of the AMLCFT Law, the maximum penalty for violating the Sanctions List is AED 5 million, whereas an FI can be fined up to AED 10 million for the same offence.

6.8 There are other potential consequences from a civil law perspective.

There is no limitation in principle to other potential consequences for a violation of civil economic sanctions. Other potential consequences may vary depending on the nature of the violation and required measures to avoid a breach of sanctions, including the seizing and destruction of assets and freezing of bank accounts. Notably, pursuant to Article 22 of the New Sanctions Regulations, the supervisory authorities have been provided wide jurisdiction to "conducting supervision, control, and follow-up to ensure compliance with the provisions stipulated in [the New Sanctions Regulations] through office and field inspections and imposing appropriate administrative penalties upon violating or failing to implement them".

Certain companies involved in money laundering and proliferation of dual-use/dangerous materials have had their trade licenses revoked due to breach of the AMLCFT Law, sanctions regulations, Commodities as well as the Non-Proliferation Treaty and other UN resolutions.

6.9 The civil enforcement is process, including the assessment of penalties.

Are all resolutions by the competent authorities' public?

Assessment of penalties depends on the breach itself. Where the latter includes a transaction, the penalty can be linked to the value of the transaction. Should a matter be brought before the courts, the penalty assessment can also be left to the discretion of the judge. Not all resolutions by the competent authorities are public; certain penalties are imposed at their discretion and are based on the gravity of the violation.

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".

III. Requirements from Financial Institutions

- Mechanism to screen customers at the time of on-boarding
- Mechanism to screen customers at the time of transactions whenever possible
- Mechanism to screen the customer database when the lists are updated (Notified by the FIU)
- Be vigilant about the transactions for high-risk customers (from high-risk countries)
- Increase awareness of the staff about the screening requirements.

IV. Enhanced Scrutiny of High-Risk Customers and Transactions

Who are high risk customers?

- Customers from DPRK, Iran or their neighboring countries
- Who may act on behalf of or at the direction of DPRK and Iran?

Who provides trade services?

- To Iran, DPRK, or countries neighboring them
- To countries that have weak AML/CFT/CPF controls
- For dual use items

V. Additional information obtained for high-risk customers and transactions

- purpose of transaction or payment
- details about the nature, end use or end user of the item
- parties to the transaction
- sources of funds
- beneficial ownership of the counterparty
- export control information (copies of export-control or other licenses issued by the national export control authorities, and end-user certification)
- information in accordance with wire transfers

VI. Elements that may Indicate Proliferation Financing

- Person or entity in Iran, DPRK or its neighboring countries
- Altering transaction originator information, especially in EFTs
- Person or entity is “listed” or has a history of export control contraventions
- Customer activity doesn’t match profile
- A freight forwarding firm is listed as the product’s final destination
- Order from one country, end user in another country
- Shipment incompatible with the technical level of the shipped country
- Circuitous route of shipment and/or circuitous route of financial transaction
- Shipment route through country with weak import/export control laws
- Shipments inconsistent with normal geographic trade patterns

VII. Elements that may Indicate Proliferation Financing

- Declared value of shipment seems under-valued vis-à-vis the shipping cost
- Customer vague/incomplete/resistant on information it provides
- Payment instruction to parties not identified on the original trade documents
- Involvement of items controlled under WMD export control regimes
- Person dealing with complex equipment for which he/she lacks technical background
- Involvement of a small trading, brokering or intermediary company
- Involvement of a university in a country of proliferation concern
- Vague description of goods
- 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

VIII.Consequences of Non-compliance

- Imprisonment and/or fines
- Reputational damage
- Suspension of business

7 What is a sanction?

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.

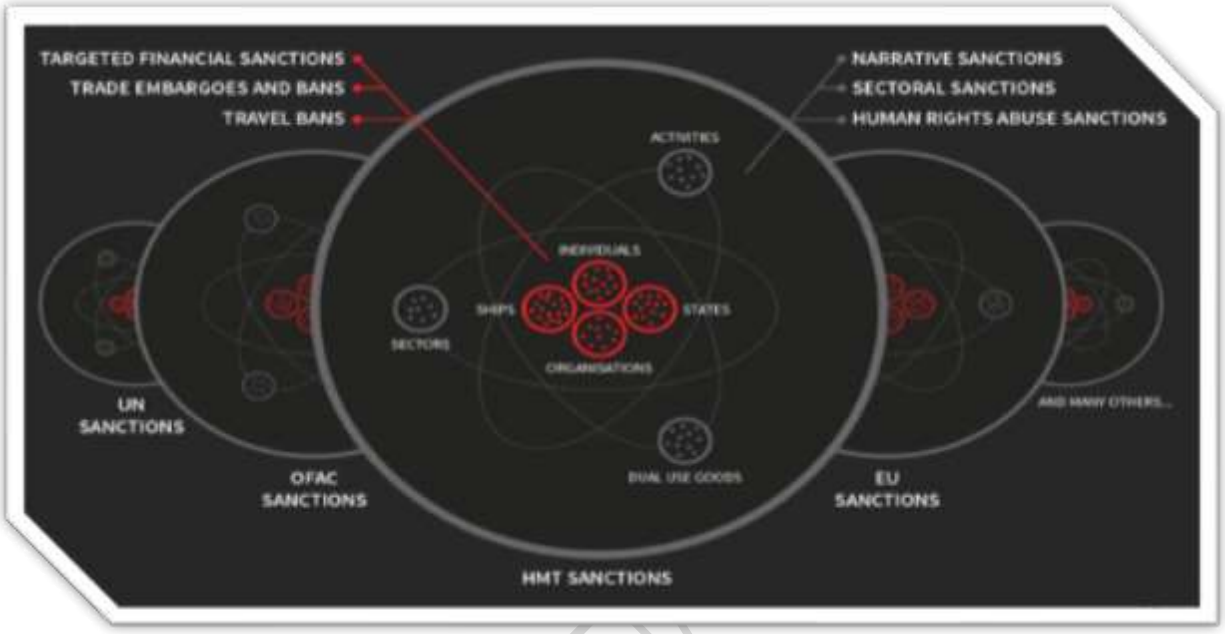
7.1 What is a sanctions list?

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.

7.2 Managing sanctions risk has never been so complex

- 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.
- 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.
- 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 sanctions 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.



7.3 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.

I. 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.

II. 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.

III. 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.

IV. UN Sanctions

The United Nations Security Council sanctions list applies to:

- All UN Nation states.

7.4 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.

7.5 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.

7.6 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.

7.7 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.

7.8 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:

- **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 cable 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.

- **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.

- **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 rein stance 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.

7.9 Tips for effective sanctions screening

- **Prepare your customer data well:**

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.

- **Use proven, reliable technology to support sanctions screening.**

Solutions should be capable of handling multiple lists, batch screening, and be able set up predefined searches tailored to an organizations risk exposure and policies.

- **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.

i. 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.

ii. 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 trial, evidencing for both regulators and internal stakeholders that adequate procedures have been followed.

iii. 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.

8 Sanctions Compliance Program

FALCON PRECIOUS METAL REFINERY (FZC) 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.

FALCON PRECIOUS METAL REFINERY (FZC) 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.

9 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.

10 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.

11 Risk Assessment

FALCON PRECIOUS METAL REFINERY (FZC) 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.

12 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.

13 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.

14 Policies and Procedures

FALCON PRECIOUS METAL REFINERY (FZC) 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.

15 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.

16 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 because 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.

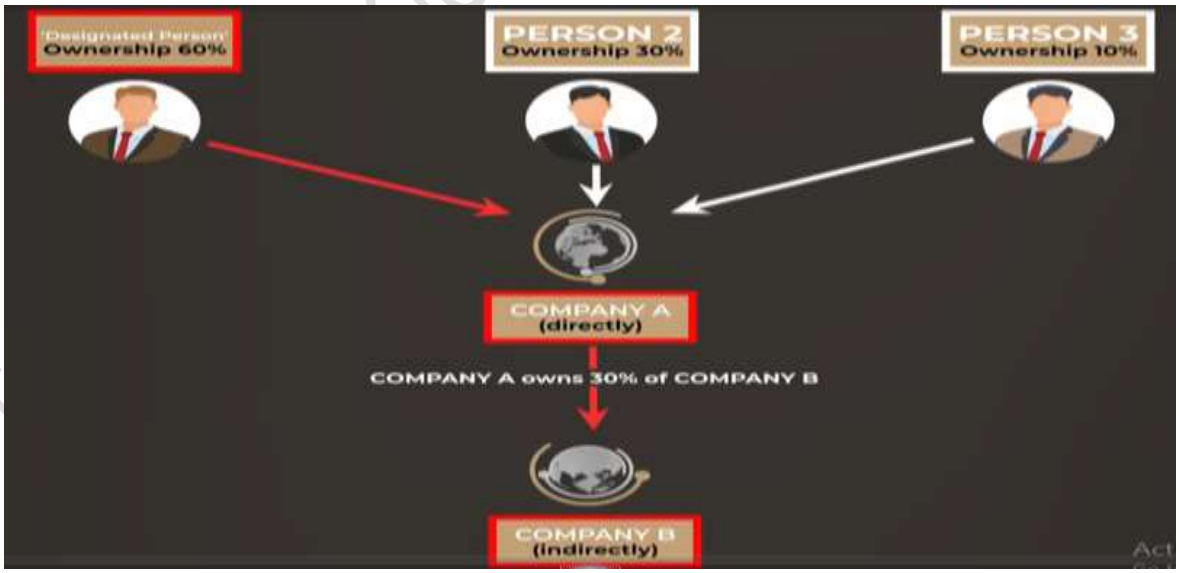
17 Record Keeping

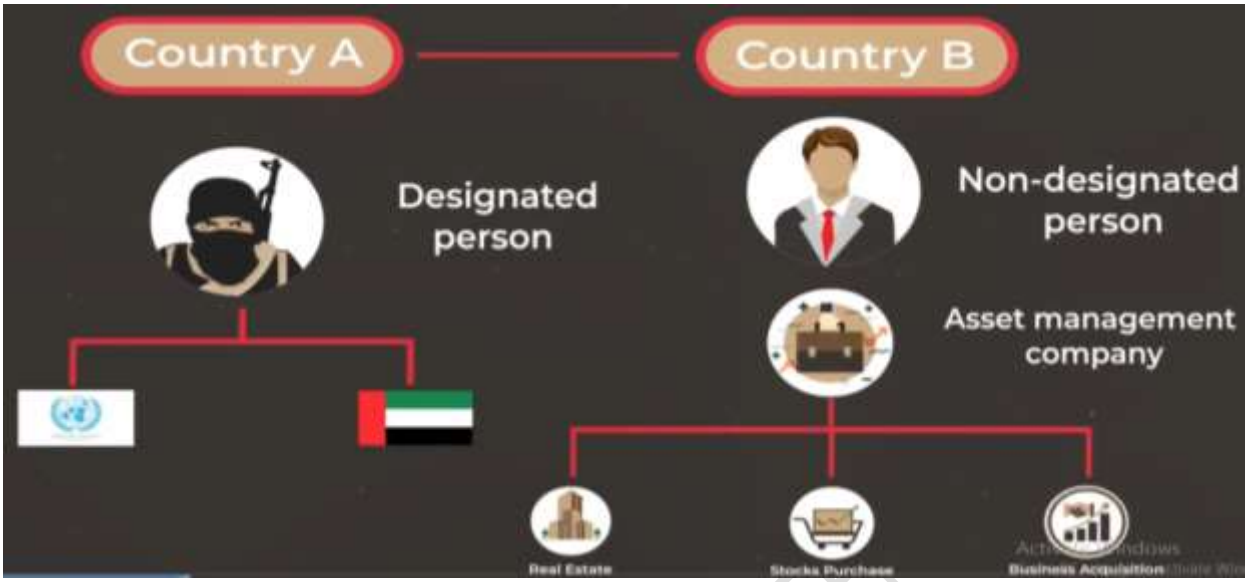
According to the AML-CFT Law and the AML-CFT Decision, company must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as all records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the 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.

18 Steps to implement Targeted Financial Sanctions

Any individual or entity designated by the **United Nation's Security Council** for proliferation financing in relation to UNSCR 2231 and UNSCR 1718





In compliance with
Cabinet Resolution No. 74 of 2020,
all natural and legal persons should apply the following steps to implement Targeted Financial Sanctions.

18.1 Screening Operations

Under Article 21.2 of Cabinet Decision 74, Company must regularly screen their databases and transactions against names on the UN Consolidated List and the Local Terrorist List, and also immediately when notified of any changes to any of such lists, provided that such screening includes the following:

- Searching their customer databases
- Search for the names of parties to any transactions
- Search for the names of potential customers
- Search for the names of beneficial owners
- Search for names of persons and organizations with which they have a direct or indirect relationship.
- Continuously search their customer database before conducting any transaction or entering into a serious business relationship with any person, to ensure that their name is not listed on the UN Consolidated List or the Local Terrorist List.

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

For natural person
• Name • Aliases • Date of birth • Nationality • ID or passport information • Last known address

For legal persons
• Name(s) • Aliases • Adddress of registration • Address of branches • Other information

Potential match	A potential match is when there is a partial match between identifiers in the Sanctions Lists with any information in your databases, and you are unable to conclude a false positive or a confirmed match.	**Example:** Your customer's name and DOB match with the identifiers of a designated person in the Sanctions Lists, but the nationality is different and there is a slight difference in the name spelling.

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

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

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

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

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

18.2 Apply Targeted Financial Sanctions

The obligations to freeze without delay shall not prevent additions to frozen accounts of:
The following are the TFS measures that must be implemented if a match with the Local Terrorist List or UN Consolidated List is identified.

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

- Interest, profits, or other earnings due on the account; or

- Of payments due under contracts, agreements or obligations agreed upon prior to the date on which the account has become subject to freezing, provided such additions are immediately frozen

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

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

18.3 Sanctions Evasion

Illicit actors targeted by sanctions are likely to utilize a range of tactics to evade prohibitions, which can be difficult to identify. Companies should remain vigilant in order to identify attempts to evade, avoid, or circumvent sanctioned activities. Frequent tactics employed for sanctions evasion include renaming, using intermediaries, creating front companies, and using alternative financial networks. LFIs should monitor not only for sanctions violations but also for red flags of potential evasion risks. Company also a need to remain vigilant for new methods of evading sanctions. Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") play a critical role, in combination with sanctions screening, to identify and prevent more complicated forms of sanctions evasion.

Companies should also prohibit activity that aims to evade or circumvent sanctions prohibitions. Accordingly, company must not engage in activities that could be part of a sanction's evasion scheme, including but not limited to:

- Tipping off customers or counterparties;
- Omitting, withholding, altering, misstating, or removing any information about customers or transactions;
- Accepting incomplete (when the customer deliberately does not provide an identifier to obscure being matched with the sanctions lists, such as a date of birth or address) or false information (when the customer provides a false identifier that would not match with the sanctions lists listed details, such as a wrong date of birth);
- Providing false or incomplete information to counterparties or sanctions-imposing authorities; or
- Any other activities that would cause a conflict with or failure to comply with this Guidance.

18.4 Maintenance of UN Consolidated List and Local Terrorist List

Company should rely on the official website of the UNSC for the most updated UN Consolidated List:
https://www.un.org/securitycouncil/content/un-sc-consolidated-list

Company should rely on the official website of the Executive Office to obtain the most recent publication of the Local Terrorist List issued by the UAE Cabinet:
https://www.uaeiec.gov.ae/en-us/
https://www.uaeiec.gov.ae/ar-ae/

In addition, under Article 21 of Cabinet Decision 74, Company must register on the Executive Office's website in order to receive automated email notifications with updated and timely information about the Listing and de-Listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List.

When company utilize external vendors' lists for their Sanctions List and Local Lists, it is the company responsibility to undertake due diligence on these vendors and ensure that the vendors' lists contain all names listed by the UN Consolidated List and UAE Local Terrorist List.

18.5 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.

18.6 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:

i. **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.

ii. **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.

iii. **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. LFIs should perform their own assessments on whether to screen for weak aliases based on their understanding of their own risk profile.

18.7 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”.

18.8 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.

18.9 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.

19 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.

19.1 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.

19.2 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.

i. 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.).

ii. 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.

iii. 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.

20. Partial Name Match Report & Funds Freeze Report

- Reporting Requirements
- Procedures : In line with the recent Supervisory Authorities communications on the subject and the obligation for TFS reporting, as stipulated in the Cabinet Decision (74) of 2020 "Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions", two new reports have been introduced into goAML for Reporting Entities (REs) to use in this regard:

1. **Funds Freeze Report (FFR)**: To be used to report any freezing measure, prohibition to provide fundsor services, and any attempted transactions related to 'confirmed matches'.
2. **Partial Name Match Report (PNMR)**: To be used to report any 'potential match'.

Additionally, the following Reason for Reporting (RFRs) have been created to be used with these reports. FALCON PRECIOUS METAL REFINERY (FZC) asked to use the correct and most applicable Reasons for Reporting (RFRs) when submitting the afore mentioned report types via goAML.

1. TFS/PFS – Domestic list
2. TFS/PFS - UNSCRs

FALCON PRECIOUS METAL REFINERY (FZC) is expected to take all measures required as per cabinet decision (74) of 2020 in line with the procedures or guidance received from their supervisory authorities.

FALCON PRECIOUS METAL REFINERY (FZC) should consult the published guidelines issued by their supervisory authorities and theExecutive Office - IEC published guidelines, respectively, as updated from time to time in this regard.

A link to the Executive Office - IEC's website is found herein: https://www.uaeiec.gov.ae/en-us/un-page

For technical queries related to goAML, please contact the goAML Support team goaml@uaefiu.gov.ae

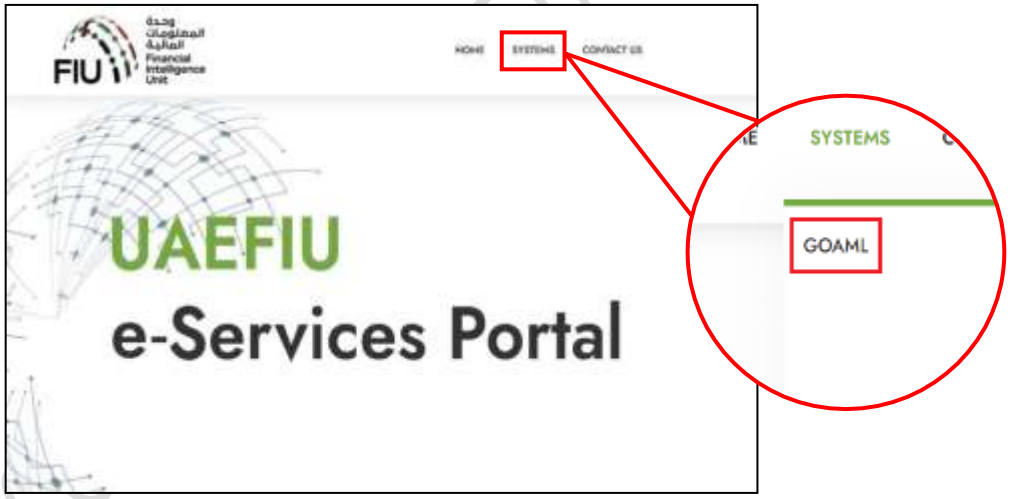
For any queries related to the implementation of TFS, please contact the Executive Office - IECiec@uaeiec.gov.ae and your Supervisory Authority.

Accessing goAML

FALCON PRECIOUS METAL REFINERY (FZC) can access the goAML by utilizing the username and password they created during theregistration process. However, FALCON PRECIOUS METAL REFINERY (FZC) registration requests should be approved by their respective regulator before the registering organization is on-boarded to the goAML. Such always be required before FALCON PRECIOUS METAL REFINERY (FZC) is to granted access to the goAML.

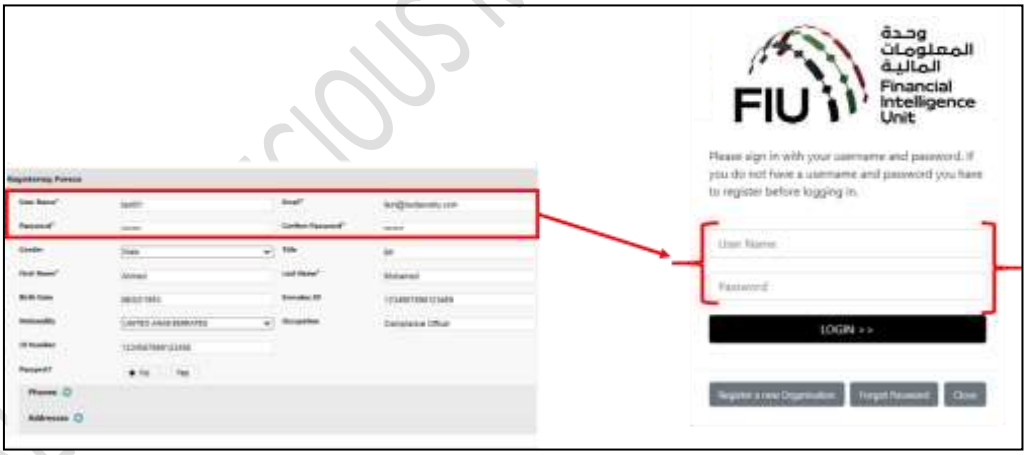
Login Process

1. Click on the **Login** link https://services.uaefiu.gov.ae
2. Navigate to **Systems**
3. Click on **GOAML**



4. You will then see the below pop-up screen; where you need to use the username received fromno-reply.sacm@uaefiu.gov.ae and the Google Authenticator Passcode as the password.
5. You will be directed to the goAML homepage.
6. Click the Login Button

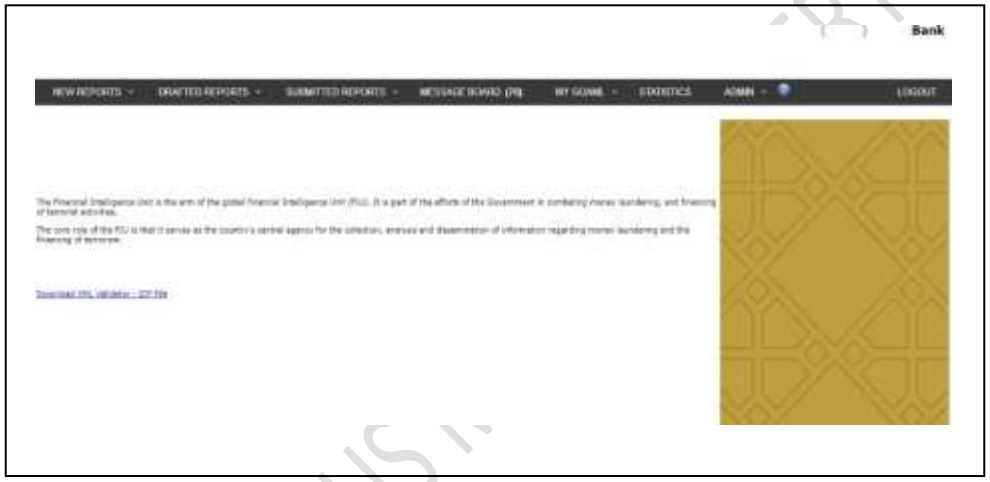
7. Type in the username and password you created at the time of registering on goAML then click login.



goAML Platform Landing Page

The landing page has the following visible items

- **Logged in user details** - displays the username and the corresponding institution name (e.g. Ali from Gulf Global Bank).
- **Menu Bar** - contains New Reports / Drafted Reports / Submitted Reports / Message Board / My goAML / Statistics / Admin, clicking any of the link items will give a user access to the required functionality (e.g. clicking message board populates the message board).
- **Logout –** allows the user to logout.



20.1 Submitting a PNMR or FFR

Submission Options

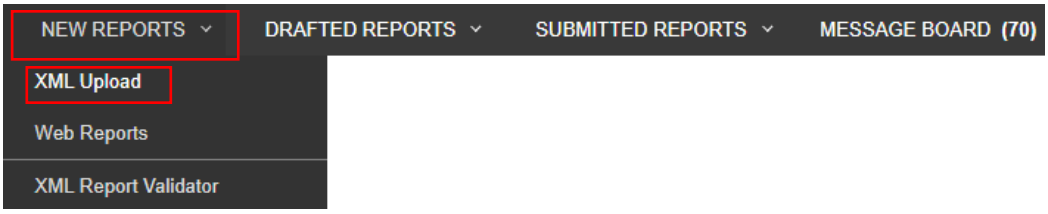
The goAML system allows users to submit a report through the following options :

XML Reports

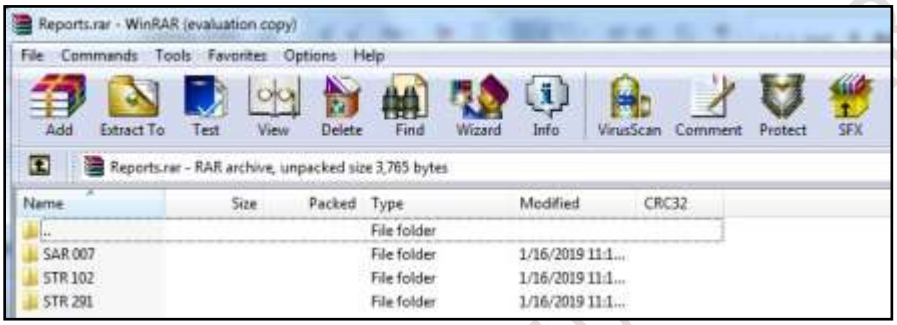
If the FALCON PRECIOUS METAL REFINERY (FZC) has goAML- compliant XML files, then they may simply upload them to the goAMLby uploading individual XML report files or XML reports in a ZIP file.

The link for uploading reports is accessible by hovering the mouse pointer on the menu bar:

- **New Reports** > select **XML Upload**



- Click on **Browse** and select the XML file to be uploaded. The user can select either a single XML file or a zipped file. In case of a zipped file, the user may enter multiple XML files along with attachments granted that they are in the appropriate format as depicted below:



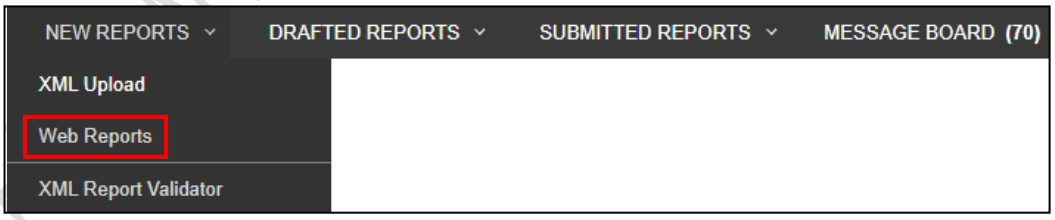
- Click on **Upload**. The data is then uploaded to the goAML for acceptance or rejection.

➢ Web Reports

If the FALCON PRECIOUS METAL REFINERY (FZC) wishes to submit a report but does not have the data available in XML format, then they may enter the report directly onto a web form available on the goAML platform.

The link for uploading reports is accessible by hovering the mouse pointer on the menu bar:

- **New Reports** > select **Web Reports**

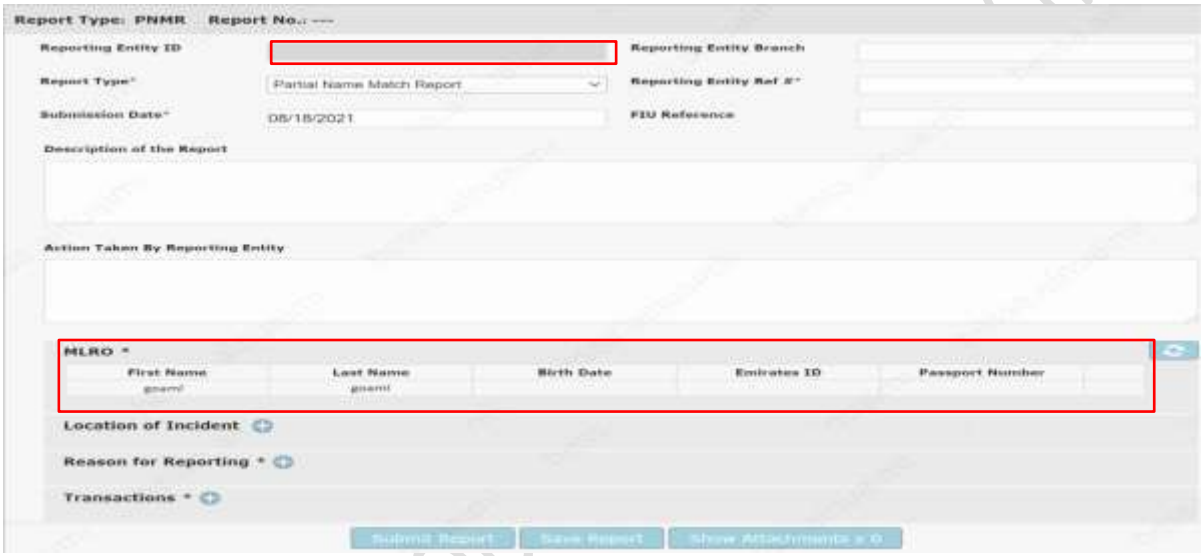


Once selected, a new general reporting template will be generated which will be discussed in detail in the following sections.

20.2 How to submit a PNMR & FFR

An Overview of the Report Cover

The form for creating new reports is loaded and displayed. Kindly note the form fields **'Reporting Entity ID'** and **'MLRO'** are auto-populated and cannot be changed. The Reporting Person details are linked to the logged in user details. Kindly note that all fields denoted with an asterisk (*) in the goAML are mandatory and must be completed in order to submit the report. Additional fields that are not denoted with an asterisk, are mandated. Please refer to the Business Rejection Rules (BRRs) for more information.



Select the Report Type

The report type to be submitted can be selected from the **'Report Type'** drop-down menu.

- To submit a report, open the '**Report Type'** drop-down menu and select the type of the reportyou want to file, "**Partial Name Match Report**" or "**Funds Freeze Report**".

After selecting the "Partial Name Match Report" or the "Funds Freeze Report" option, the MLRO may now proceed with populating all available details in the Report Cover as depicted below:

- **Reporting Entity ID** – Entity name as per the registration (auto-generated)
- **Report Type*** – Kindly select the relevant report. “Partial Name Match Report” or “Funds Freeze Report”.
- **Submission Date*** – Date of submitting the report to the FIU (auto-generated)
- **Description of the Report*** – Kindly provide adetailed description for the suspicions and reason for submitting this report to the FIU.
- **Reporting Entity Branch** – Branch where the main subject(s) of the report were identified.
- **Reporting Entity Ref #*** – Internal report reference number i.e. the reference numberassigned to this report within your organization
- **FIU Reference** – *Only applicable in the case of AIF/RFI/AIFT/RFIT reports*. Kindly quote the corresponding case number as specified in the Message Board communication sent by the FIU.
- **Action Taken by Reporting Entity*** – The action(s) taken by the FALCON PRECIOUS METAL REFINERY (FZC) post-identifying the reason for suspicion/submission.

20.3 Saving / Submitting the Report

- **Submit Report** - Reports can be submitted using the Submit Report Button.
- **Save Report** - Save the reports for editing later.

- **Show Attachments –** documents can only be attached after saving the report, this button must be used to attach documents such as identification document (ID), proof of address, deposit slips,multimedia files and client information. Please note that each attachment should be a maximumof 5 MB, and a total of 20 MB is allowed per report. Attachment file names should be short and should not contain any special characters.

It is important to note that documents are mandatory for submitting PNMRs and FFRs to provethe potential name match and/or proof of fund freeze.

For the full list of **Business Rejection Rules,** please refer to the hyperlink on the goAML web homepagenamed the same.