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

Terrorist and Proliferation Financing
Red Flags Guidance

Published: September 2023
Updated: December 2023

Contents

Acronyms

DNFBPs	Designated Non-Financial Businesses & Professions
DPMS	Dealers in Precious Metals & Stones
DUG	Dual-use goods
FATF	Financial Action Task Force
FIs	Financial Institutions
PF	Proliferation Financing
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UBO	Ultimate Beneficial Owner
UNSCRs	United Nations Security Council Resolutions
VASPs	Virtual Asset Service Providers
WMD	Weapons of mass destruction

Section 1: Introduction and Purpose

1. The purpose of this document is to provide a consolidated list[1] of Terrorist Financing (TF) and Proliferation Financing (PF) red flags that aim to assist financial institutions (FIs), designated non-financial businesses & professions (DNFBPs), and virtual asset service providers (VASPs) in identifying and detecting suspicious TF and PF activities, including those that may be related to the evasion of targeted financial sanctions (TFS) imposed under United Nations Security Council Resolutions (UNSCRs) or by local designations.

2. **Sanctions evasion** is an attempt by designated persons to circumvent the targeted financial sanctions imposed on them under relevant UNSCRs or by local designations through the use of multiple evasion tactics, such as renaming, use of intermediaries and front companies, and using alternative financial networks with the aim of accessing funds and other assets and services.

3. The document also aims to raise awareness among FIs, DNFBPs, and VASPs, and to strengthen their internal control and oversight systems to detect cases of sanctions evasion related to the financing of terrorism or the proliferation of weapons of mass destruction (WMD) and to report them in accordance with the reporting requirements detailed in Section 2.

Section 2: Reporting Suspicious TF and PF Activities

4. Article 15 of Federal Decree-law No. (20) of 2018 On Anti-Money Laundering And Combating The Financing Of Terrorism And Financing Of Illegal Organisations (amended by Federal Decree Law No (26) of 2021 to amend certain provisions of Fedreral Decree Law No (20) of 2018) and Section 5 of Cabinet Decision No. (10) of 2019 Concerning The Implementing Regulation Of Decree Law No. (20) Of 2018 On Anti- Money Laundering And Combating The Financing Of Terrorism And Illegal Organisations (CD 10) set out the legal obligations on FIs, DNFBPs, and VASPs with respect to reporting suspicious transactions and activities.

5. FIs, DNFBPs, and VASPs are required to file a suspicious transaction report (STR) or suspicious activity report (SAR) to the UAE Financial Intelligence Unit (FIU) when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds

[1] While this document aims to provide a consolidated list of red flag indicators, it may not provide a comprehensive list and may be updated occasionally by addition of new red flag indicators.

constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime.

6. STR/SAR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. STR/SAR filings are essential to assisting law enforcement authorities in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

7. In addition to the obligation of reporting suspicious transactions and activities, Article 16 of CD 10 requires FIs, DNFBPs, and VASPs to put in place indicators that can be used to identify suspicions that may indicate illicit activities and update those indicators on an ongoing basis. **As such, it is recommended that FIs, DNFBPs, and VASPs update their screening systems with the latest red flags and indicators in order to be able to better identify and detect unusual or suspicious transactions and activities.**

8. For more information on submitting STRs/SARs, please refer to the goAML Web Report Submission Guide available on the FIUs website.

Section 3: TF and PF Red Flags

9. Global standards-setters have identified "red flag" indicators to help FIs, DNFBPs, and VASPs detect activities related to TF and PF.

10. Such "red flag" indicators suggest the likelihood of the occurrence of unusual or suspicious activity, including possible PF activities, money laundering (especially trade- based money laundering), terrorist financing, and evasion of TFS.

11. The existence of a single standalone indicator may not on its own warrant suspicion of TF, PF, or a TFS evasion attempt, nor will a single indicator necessarily provide a clear indication of such activity, but could prompt further monitoring and examination, including the application of customer or transactional enhanced due diligence, as appropriate.

12. The consolidated list of TF and PF red flags can be found below.

TF Red Flags

13. The following red flags are specific to terrorist financing cases **related to the UAE and other regional countries**:

- 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[2].

- Funds are sent or received via international transfers from or to higher-risk locations.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.
- Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries, particularly in higher-risk locations.
- Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.
- An individual or entity's online presence supports violent extremism or radicalization.
- Irregularities during the CDD process which could include, but is not limited to:
    - Inaccurate information about the source of funds and/or the relationship with the counterparty.
    - Refusal to honor requests to provide additional KYC documentation or to provide clarity on the ultimate beneficiary of the funds or goods.
    - Suspicion of forged identity documents.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g., crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).
- 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

[2] "Sanctioned countries" refer to countries subject to sanctions under United Nations Security Council Resolutions or related countries. For a full list of such UNSCRs, please refer to Appendix A. This footnote applies wherever references are made to sanctioned countries and/or jurisdictions.

purpose for the transfers, particularly when this activity involves higher-risk locations.

- 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 customer receives/ sends money declaring it for personal needs, but the actual purposes are for trade related transactions. The intention of the customer is to hide the underlying nature of the transaction and circumventing the regulatory requirements thereon. Further, the customer could potentially be trying to hide the details of the ultimate beneficial owner (UBO)[3] of the corporate to circumvent the possible sanctions screening detection.

- Sudden spurt in currency exchange transactions by a group of resident / non-resident customers who could be from similar geographic locations, profession, or age group, who are acting as mules to assist larger cash smuggling groups.

14. The list below covers other red flags that may be applicable to the **broader TF context**:

- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.

- Funds are 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 Financial Action Task Force (FATF) as non-cooperative countries and territories).

- Transactions involving certain high-risk jurisdictions[4] 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.

- Raising donations in an unofficial or unregistered manner.

[3] Article 5 of Cabinet Resolution No. 58 of 2020 states “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.

[4] High-risk jurisdictions may include, among other considerations, jurisdictions that are listed under the Financial Action Task Force (FATF) list of countries under increased monitoring “Grey List” or subject to a call for action “Black List”, as well as jurisdictions subject to UNSCRs.

- 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.

- 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.

- 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.

PF Red Flags[5]

15. The following red flags are specific to proliferation financing cases **related to the UAE and other regional countries:**

- Dealings, directly or through a client of your client, with sanctioned countries[6] 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 dual-use (DUG) or controlled goods[7]. For example:

    - Chemicals

    - DUG (wire nickel, inverters, etc.)

[5] In general, PF red flags may be similar in nature to trade-based money laundering due to the involvement of trade in PF activities.

[6] Sanctioned countries in a PF context include countries sanctioned under United Nations Security Council Resolutions on WMD proliferation grounds. These UNSCRs include measures to implement targeted financial sanctions on lists of designated individ- uals and entities. As of publication date, the UNSCRs that fall under this category are: UNSCR 1718 (2006) related to the Demo- cratic People's Republic of Korea and UNSCR 2231 (2015) related to the Islamic Republic of Iran.

[7] Refer to Cabinet Decision No. 50 of 2020 for the latest list of dual-use controlled items.

- Dealings with sanctioned goods or under embargo[8]. For example:
    - Weapons
    - Oil or other commodities
    - Luxury goods (for DPRK sanctions)
- Identifying documents (e.g., bill of lading, sales purchase agreement, etc.) that seem to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
- A shipment of goods is incompatible with the known business activity and nature of products or services provided by the entities involved in the transaction.
- 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 which is not in accordance with their trade license.
    - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide humanitarian aid.
- Transactions involved in sale, shipment, or export of DUG is incompatible with technical level of the country being shipped (e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- 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 UBO.

[8] Examples of sanctioned goods or under embargo include the prohibited items listed under UNSCR 1718 (2006), such as luxury goods, or the Charcoal Ban under UNSCR 751 (1992).

- The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern, e.g., DPRK and Iran.

- The use of representative offices of UNSC sanctioned banks to remit DPRK labours money to DPRK.

- The use of extensive currency exchange networks to transfer bulk cash to Iranian nuclear program.

- The use of cyber-attacks by the DPRK regime to steal funds from FIs and crypto currency exchanges.

- A trade finance transaction involves a shipment route (if available) through a country with weak export control laws or weak enforcement of export control laws.

- When the flows of funds exceed those of normal business (revenues or turnover).

- The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination.

- Based on the documentation obtained in the transaction, the declared value of the shipment is obviously undervalued vis-à-vis the shipping cost.

- A shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flag hopping, or using a small or old fleet.

- The account holder conducts financial transactions in a circuitous manner.

- The customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business.

- A customer or counterparty, declared to be a commercial business, conducts transactions that suggest that they are acting as a money remittance business or a pay-through account. These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the originators appear to be entities who may be connected with a state-sponsored proliferation programme (such as shell companies operating near

countries of proliferation or diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls.

- A transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.

- A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding.

- The transaction involves receipt of cash (or other payments) from third party entities.

- that have no apparent connection with the transaction.

- Customer activity does not match the customer's business profile, or end-user information does not match the end-user's business profile.

- Inconsistencies are identified across contracts, invoices, or other trade documents, e.g., contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions.

- Customer approaches to receive high value transactions which are initiated from high-risk jurisdictions/ bordering to high-risk jurisdictions claiming that the origin of funds are from sale of property or any other assets in the homeland. However, the actual source is not supported with adequate supporting documents and often a fake transaction.

16. The list below covers other red flags that may be applicable to the **broader PF context:**

a. Customer Profile Risk Indicators

- During onboarding, a customer provides vague or incomplete information about their proposed trading activities. The customer is reluctant to provide additional information about their activities when queried.

- During subsequent stages of due diligence, a customer, particularly a trade

entity, or its owners or senior managers, appears in sanctioned lists or negative news, e.g., relating to past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes.

- The customer is a person connected with a country of proliferation or diversion concern, e.g., through business or trade relations, as identified through the national risk assessment process or by relevant national CPF authorities.
- The customer is a person dealing with DUG, goods subject to export control, or complex equipment for which he/she lacks technical background, or that is incongruent with their stated line of activity.
- A customer affiliated with a university or research institution is involved in the trading of DUG or goods subject to export control.
- A new customer requests a letter of credit transaction while awaiting approval of a new account.

b. Account and Transaction Activity Risk Indicators

- A transaction involves a person or entity in foreign country of proliferation concern.
- A transaction involves a person or entity in foreign country of diversion concern.
- A 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.
- Wire transfer activity shows unusual patterns or has no business or apparent lawful purpose.
- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g., companies do not have a high level of capitalisation or display other shell company indicators. Countries or the private sector may identify more

indicators during the risk assessment process, such as long periods of account dormancy followed by a surge of activity.

- Business or compliance personnel identify links between representatives of companies exchanging goods, e.g., the same owners or management, physical address, IP address, or telephone number, or activities that appear to be coordinated.

- A transaction or account activity involves an originator or beneficiary that is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards or a weak export control regime (also relevant to correspondent banking services).

- The customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. For financial institutions, the transactions are visible through sudden influxes of cash deposits to the entity's accounts, followed by cash withdrawals.

- Transactions are made on the basis of "ledger" arrangements that obviate the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies that maintain a record of transactions made on each other's behalf. Occasionally, these companies will make transfers to balance these accounts.

- Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the account holders have previously violated requirements under dual-use or export control regimes.

- Use of cash or precious metals (e.g., gold) in transactions for industrial items.

- Buyer entity & seller entity are owned by the same / related UBOs and using the trade channels to launder money.

- Sudden increase in online sales by particular vendors (online auction / e-commerce sites).

- Unrelated individuals are sending remittances from foreign countries to low-income resident individuals from some unrelated nationalities, who are

acting as mules to receive money for unknown beneficiaries.

c. Maritime Sector Risk Indicators

- An order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- A trade entity is registered at an address that is likely to be a mass registration address, e.g., high-density residential buildings, post-box addresses, commercial buildings, or industrial complexes, especially when there is no reference to a specific unit.
- The destination of a shipment is different from the importer's location.
- A shipment of goods is inconsistent with normal geographic trade patterns, e.g., the destination country does not normally export or import the goods listed in trade transaction documents.
- A shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, weak export control laws, or weak enforcement of export control laws.
- Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons, e.g., by a shell or front company not involved in the trade transaction.
- The vessels stops at single or multiple high risk or sanction ports in transit.

d. Trade Finance Risk Indicators

- A transaction involves a shipment of goods inconsistent with normal geographic trade patterns (e.g., does the country involved normally export/import good involved?).
- Prior to account approval, the customer requests a letter of credit for a trade transaction to ship DUG or goods subject to export control.
- Lack of full information or inconsistencies are identified in trade documents and financial flows, such as names, companies, addresses, final destination, etc.

- Transactions include wire instructions or payment details from or due to parties not identified on the original letter of credit or other documentation.

Appendix A: United Nations Security Council Resolutions – Sanctions Regimes

Resolution	Related Country / Countries
Security Council Committee pursuant to resolution 751 (1992) concerning Al-Shabaab	Somalia
Security Council Committee pursuant to resolutions 1267 (1999) 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities	Iraq and the Levant
Security Council Committee established pursuant to resolution 1518 (2003)	Iraq
Security Council Committee established pursuant to resolution 1533 (2004) concerning the Democratic Republic of the Congo	Democratic Republic of Congo
Security Council Committee established pursuant to resolution 1591 (2005) concerning the Sudan	Sudan (Darfur)
Security Council Committee established pursuant to resolution 1636 (2005)	Lebanon
Security Council Committee established pursuant to resolution 1718 (2006)	Democratic People's Republic of Korea (DPRK)
Security Council Committee established pursuant to resolution 1970 (2011) concerning Libya	Libya
Security Council Committee established pursuant to resolution 1988 (2011)	Afghanistan (Taliban)
Security Council Committee established pursuant to resolution 2048 (2012) concerning Guinea-Bissau	Guinea-Bissau
Security Council Committee established pursuant to resolution 2127 (2013) concerning the Central African Republic	Central African Republic
Security Council Committee established pursuant to resolution 2140 (2014)	Yemen
Security Council Committee established pursuant to resolution 2206 (2015) concerning South Sudan	South Sudan

Security Council Committee established pursuant to resolution 2374 (2017) Concerning Mali	Mali
Security Council Committee established pursuant to resolution 2653 (2022) concerning Haiti	Haiti
Resolution 2231 (2015) on Iran Nuclear Issue[9]	Iran

[9] Sanctions under this resolution are imposed directly through the UN Security Council and as such this resolution does not have a Security Council Committee.

Appendix B: DPMS Red Flags

The list below comprises of red flags that are specific to the Dealer in Precious Metals & Stones (DPMS) sector in the TF / PF context:

- Customers (including bullion dealers) dramatically increasing their purchase of gold bullion (in comparison to their previous purchase pattern) for no apparent reason.
- Foreign nationals purchasing gold bullion through multiple transactions over a short time period.
- Unusual pattern and nature of bullion transactions inconsistent with the customer profile.
- A previously unknown customer from local market requesting a refiner to turn scrap/ dust/ore gold into bullion (tradable bars).
- Unusual interest to keep transactions below reporting threshold limit.
- Creation of benami companies[10] and thereby trading in different names by the same UBO. Numerous entities are set up in the name of seemingly unrelated people (proxies) but controlled by the same individual or group of people. 'Benami' (by concealing the identity of the true beneficiary/controlling person/owner) identity is used to register such businesses.
- Significant number of companies conducting the same or related business activities and registered under the name of a single individual.
- No clarity on how the company transports its merchandise after purchase.
- Gold is shipped to or from a high-risk jurisdiction.
- Gold is trans-shipped through one or more high-risk jurisdictions for no apparent economic reason.
- A number of affiliated entities in the payments chain.
- Asking for shipment of goods to countries where the company is not

[10] Benami companies are those that are created under a fictitious name or created/transacted under a name different than that of the actual owner.

registered/having no real presence.

- The use of cash to purchase bullion, especially when there are multiple purchases in a short timeframe, or when large amounts are purchased at once, or when there are structured cash deposits into an account to pay for a single gold bullion purchase.
- Transactions between domestic buyers and sellers with sales proceeds sent to unknown third parties overseas.

Appendix C: VASPs Red Flags

The list below comprises of red flags that are specific to the Virtual Asset Service Providers (VASPs) sector in the TF / PF context:

- Rapidly moving virtual assets between different virtual asset service providers, especially in different jurisdictions within a short space of time, without a clear reason.
- The use of anonymity-enhanced virtual assets [Privacy Coins], mixing services, tumblers, cross chain bridges or other means to obscure transaction history and details.
- The use of virtual assets to send funds to a few select wallets at unregulated virtual assets exchanges (or exchanges in sanctioned jurisdictions or in territories where sanctioned persons have influence).
- Transactions with other high risk virtual asset exchanges, high risk counterparties or wallets that have been flagged for previous suspicious activities.
- Transfer of virtual assets to or from addresses known to be associated with illegal activities on the dark web.
- Attempting to avoid regulatory reporting or monitoring by breaking down large virtual asset transactions into smaller amounts that fall below reporting thresholds.
- Transfer of virtual assets to a virtual asset exchange followed by a virtual asset-to-fiat conversion (either more or less) and withdrawal from the same exchange within a relatively short period of time.

Document Version

Original Publication Date: September 2023

Date	Section	Update
December 2023	Appendix C	Added new section on VASP specific red flags.