UNITED ARAB EMIRATES
MINISTRY OF ECONOMY & TOURISM

الإمارات العربية المتحدة
وزارة الاقتصاد والسياحة

Countering Money Laundering, Terrorism Financing and Proliferation Financing

Guidelines for Designated Non-Financial Businesses and Professions

Supplemental Guidance for Dealers in Precious Metals & Stones (DPMS)

March 2026

Table of Contents

1. Introduction

Pursuant to the *Federal Decree-Law No. (10) of 2025* and its Executive Regulations, *Cabinet Resolution No. (134) from 2025*, Dealers in Precious Metals and Stones (DPMS) fall under the Designated Non-Financial Businesses and Professions (DNFBP) category. While the United Arab Emirates' (UAE) Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing (AML/CFT/CPF) framework stipulate a threshold of AED 55,000 for the mandatory application of AML/CFT/CPF measures, it is essential that DPMS do not interpret this threshold as an exemption from applying risk-based AML/CFT/CPF obligations for transactions falling below the stipulated threshold.

The determination of risk stems from a thorough risk assessment and is not solely transaction driven. Thus, a risk-based approach must be applied to every aspect of the entity's business activity wherein the nature, pattern or context of the business relationship or transaction elevate money laundering, terrorism financing or proliferation financing risks. While the AED 55,000[1] threshold determines when a transaction becomes a "covered transaction" under UAE law and therefore triggers the mandatory application of full AML/CFT/CPF measures, this threshold does not exempt DPMS from taking appropriate, proportionate, risk-based measures below the threshold whenever the nature, pattern or context of a transaction indicates elevated ML/TF/PF risk. Thus, DPMS must therefore treat the threshold as a minimum legal trigger, while applying risk-based judgement at all transaction values. It is imperative that sector entities demonstrate a reasoned, risk-based decision-making process that is commensurate with nature of business and risks identified.

The 2024 UAE National Risk Assessment (NRA) identifies the DPMS sector as one with a high inherent exposure to money laundering risks. Yielding a residual risk rating of medium-high, the Precious Metals and Stones (PMS[2]) sector's exposure stems from a combination of factors, owing primarily to its operational environment, which is characterized by high cash intensity, portability of intrinsic high-value goods, extensive cross-border trade, involvement of legal persons and use of intermediaries. More specifically,

- PMS represent high intrinsic value in a relatively compact form, tend to maintain (or even increase) value over time, and can be easily transported physically in many forms.
- PMS can be used both as means to generate criminal proceeds (i.e. through various predicate offences), as well as vehicles to launder them.
- PMS can be used for illicit purposes, including ML/TF/PF, in a variety of ways, either directly (through physical exchange, as a form of currency) or indirectly (through exchange of value via various formal and informal financial systems, as well as via international trade and the financial products and services related to it).
- There are large, well-established, decentralised, and often cash-based markets for certain types of precious metals and stones (particularly for gold and diamonds, but for other PMS as well), often allowing them to be traded or exchanged with relative anonymity.
- The difficulty in tracing specific items, and the global nature of the markets for PMS, make it easier for criminals to exploit cross-border, multi-jurisdictional situations in order to obscure paper and money trails, while at the same time rendering it more difficult for national law enforcement authorities to detect and investigate cases.
- The scale and diversity of small and mid-sized participants in the markets for precious metals and precious stones, and the generally low level of awareness and education among them regarding ML/TF/PF risks, due-diligence requirements, and red-flag indicators associated with their trade, increase the vulnerability of DPMS to exploitation by criminal actors.
- Further complicating the risk landscape is the fact that in certain geographic regions, the buying and selling of PMS (and particularly of gold, silver, and diamonds) is a common cultural practice, often making it difficult to distinguish between legitimate transactions and their illicit counterparts.

Consequently, the sector is exposed to key money laundering threats that include trade-based money laundering (TBML), smuggling, laundering of proceeds from drug trafficking and foreign corruption and activities of professional money laundering networks. While the 2024 NRA has not identified any misuse of the sector for terrorism financing, the characteristics of the sector, as outlined above, deem it vulnerable to misuse for illicit value transfer, sanctions evasion and proliferation, especially through trade-based activities that include degrees of opacity.

[1] reports-faqs-v1-2-29-apr-2024.pdf
[2] For the sake of convenience, the abbreviations PMS and DPMS will be used throughout the text of this Supplemental Guidance to indicate the terms "precious metals and stones" and "dealers in precious metals and stones", respectively. This is without prejudice to any abbreviations or terminology which may be used to describe these goods and the persons who deal in them as provided for in any legislative or regulatory acts published, or to be published, by the Government of the UAE.

The 2024 Sectoral Risk Assessment (SRA) undertaken by the Ministry of Economy and Tourism (MoET) highlights bullion trading, refinery and wholesale activities as higher-risk subsectors because of heightened opacity in the origin of goods, complexity of supply chain that spans across jurisdictions, reliance on intermediaries and non-standard payment mechanisms. Thus, highly effective and demonstrable risk mitigation measures that are proportionate to the business activities and risk environment is expected from entities operating in these subsectors.

In view of the risk environment of the sector, this Supplementary Guidance complements the *Guidelines for Designated Non-Financial Businesses and Professions* issued by MoET by providing practical sector-specific guidance on the understanding and identification of ML, TF and PF risks and their mitigation measures, in line with the legal obligations set forth through the UAE's regulatory framework which are aligned with the Financial Action Task Force (FATF) standards.

This document must be read and implemented with a risk-based perspective; requirements indicated by "shall/must" are compulsory and "should" signifies recommended practice unless a recorded, risk-based justification supports an alternative that provides equal or greater control. In cases of any discrepancies, the Federal Decree Law, Cabinet Resolutions, and directives from the Competent Authority take precedence. Sector entities should maintain records, document decision-making processes, and regularly evaluate compliance programs to address emerging risks (such as virtual-asset exposures), supervisory input, and modifications in their business model.

1.1. Purpose and Scope

The purpose of this Supplemental Guidance is to provide guidance and assistance to regulated entities that fall under the DPMS category, in order to provide better understanding and effective implementation of applicable statutory obligations under the legal and regulatory framework in force in the UAE.

This Supplemental Guidance has been prepared by MoET and sets out minimum expectations regarding the factors that should be taken into consideration by each supervised DPMS, when identifying, assessing and mitigating the risks of money laundering, terrorism financing and proliferation financing. These expectations align with, and are intended to complement, the existing legal and regulatory framework in force.

This Supplemental Guidance is not intended to limit, replace or otherwise affect the applicability of additional circulars, notifications, memoranda, communications, or other forms of guidance or feedback (whether direct or indirect) that may be published periodically by any relevant authority in relation to regulated entities within the respective jurisdictions, or to any specific regulated entity.

DPMS must refer to and comply with the comprehensive guidelines on AML/CFT/CPF issued by MoET. This Supplemental Guidance does not duplicate provisions in the comprehensive guidelines, rather it provides sector-specific expectations, risk factors and practical considerations relevant to the unique characteristics of the DPMS sector. The general requirements therein are to be applied together with the additional sector-specific guidance outlined here, using a risk-based approach proportionate to the business activity.

It should be noted that, while this document provides high-level guidance on TFS and CPF obligations, all operational, procedural and implementation requirements remain governed by the applicable Executive Office for Control and Non-Proliferation (EOCN) guidelines.

Dealers in Precious Metals and Stones should refer to the full TFS guidelines issued by the Executive Office for Control and Non-Proliferation (EOCN), which detail their obligations under *Cabinet Decision No. (74) of 2020*, including requirements for screening, freezing, and reporting in relation to designated persons or entities.

Additionally, entities within the DPMS sector should also refer to the *Guidance on Counter Proliferation Financing Institutions (FIs), Designated Non-financial Businesses and Professions (DNFBPs) and Virtual Assets Services Providers (VASPs)* and the *Guidance on Proliferation Financing Institutional Risk Assessment* issued by EOCN to gain understanding of obligations pertinent to CPF measures and to incorporate PF risk in their Business Risk Assessment (BRA).

1.2. Applicability

Unless otherwise noted, this Supplemental Guidance apply to all Dealers in Precious Metals and Sones, and the members of their boards of directors, management and employees, established and/or operating in the territory of the UAE and Commercial Free Zones, whether they establish or maintain a Business Relationship with a Customer, or engage in any of the financial activities and/or transactions or the trade and/or business activities outlined in Articles (2) and (3) of *Cabinet Decision*

No. (134) of 2025 Concerning the Executive Regulations of Federal Decree-Law No. (10) of 2025 Concerning Combating Money Laundering, Terrorist Financing, and the Financing of the Proliferation of Weapons.

1.3. Legal Status

This Supplementary Guidance serves as a practical tool to assist regulated entities in effectively implementing the relevant crime-combatting measures and are intended to be read in conjunction with the relevant laws, cabinet decisions, regulations and regulatory rulings which are currently in force in the UAE. However, it does not constitute additional legislation or regulation, and is not intended to set legal, regulatory, or judicial precedent. Regulated entities are reminded that the Supplemental Guidance does not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. Specifically, nothing in this Supplemental Guidance should be interpreted as providing any explicit or implicit guarantee or assurance that the Supervisory or other Competent Authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws, regulations, or regulatory rulings.

This Supplemental Guidance, and any lists and/or examples provided in it, are not exhaustive and do not set limitations on the measures to be taken by regulated entities to meet statutory obligations under the legal and regulatory framework currently in force. As such, this Supplemental Guidance should not be construed as legal advice or legal interpretation. Regulated entities should perform their own assessments of the manner in which they should meet statutory obligations and should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to circumstances.

1.4. Summary of AML/CFT/CPF Obligations for Dealers in Precious Metals and Stones

Pursuant to *Federal Decree Law No. (10) of 2025* and *Cabinet Resolution (134) of 2025*, entities within the DPMS sector must fulfil AML/CFT/CPF obligations set forth, that collectively form the basis of an effective risk-based AML/CFT/CPF programme. These obligations are designed to prevent sector misuse for ML, TF or PF purposes. The sector is identified as presenting high inherent risk, as outlined in the NRA and SRA, underscoring the importance of well-implemented mitigating measures.

In line with the associated risk scoring, entities are required to fulfil the following obligations:

- *Compliance Administration* – Entities must put in place an adequate AML/CFT/CPF governance framework which consists of the appointment of a qualified Compliance Officer (CO) / Money Laundering Reporting Officer (MLRO), staff training and screening mandates, subjecting the AML/CFT/CPF framework to independent audit and overall oversight by senior management, assuming responsibility for AML/CFT/CPF compliance, in line with *Section 7* of the *Guidelines for Designated Non-Financial Businesses and Professions*. Where DPMS are part of a group, they shall implement group-wide AML/CFT/CPF programmes (policies, consolidated risk assessment, intra-group information-sharing and controls).
- *Risk Identification & Assessment* – Exposure to ML, TF and PF risks is to be identified, assessed and documented in line with *Section 8* of the *Guidelines for Designated Non-Financial Businesses and Professions*. This entails undertaking a BRA that is proportionate to the nature, size and complexity of the entity's activities as well as the risk landscape of the activities and the sector in which it operates.
- *Policies, Procedures and Internal Controls* – On the basis of the risk assessment outcome, the entity must establish, document, implement and regularly update AML/CFT/CPF policies and procedures tailored to the entity's specific business model and risk exposure with explicit measures to mitigate identified risks, in line with *Section 9* of the *Guidelines for Designated Non-Financial Businesses and Professions*.
- *Customer Due Diligence (CDD) and Ongoing Monitoring* – Entities must maintain adequate risk-based customer due diligence and ongoing monitoring procedures, in line with *Section 9* of the *Guidelines for Designated Non-Financial Businesses and Professions*. These procedures must address key areas such as the identification and verification of customers and beneficial owners, intended nature / purpose of business transactions and business relationships, creation and maintenance of customer risk profiles and application of Enhanced Due Diligence (EDD) measures where higher risks are identified. It is imperative that entities apply a risk-driven CDD and EDD measure as opposed to a threshold-driven measure so that reliance on transaction value alone does not result in the overlooking of material risk indicators. Additionally, entities must adopt an approach for dealing with

Politically Exposed Persons (PEPs), cognizant that foreign corruption is identified as one of the key ML threats in the 2024 NRA.

- *Sanctions Compliance* – Entities must comply with the directives issued by Competent Authorities of the UAE in relation to the United Nations Security Council Resolutions (UNSCR), inclusive of obligations relating to terrorism lists, targeted financial sanctions (TFS) and proliferation financing controls.
- *Suspicious Activity / Transaction Reporting (SAR/STR)* – Entities must identify and promptly report any suspicion that arises in relation to transactions and/or business relationships, in line with *Section 10* of the *Guidelines for Designated Non-Financial Businesses and Professions*. The timeliness of SAR/STR reporting and quality of these reports continue to be key supervisory focus areas for the DPMS sector.
- *Record-Keeping* - Entities must establish and maintain comprehensive records covering all transactions, CDD documentation, business correspondence, and outcomes of any analysis performed. Records must also encompass documentation generated as part of the entity's ML/TF/PF risk assessment and mitigation processes, in accordance with the requirements set out under the Executive Regulations. As outlined in *Section 11* of the *Guidelines for Designated Non-Financial Businesses and Professions,* records are to be retained for at least five (5) years from the latest of the following events:
    - The termination of a business relationship or closure of a customer account.
    - Completion of an occasional transaction where no business relationship exists.
    - The issuance of a final judgment by a competent judicial authority.
    - Dissolution, liquidation, or termination of a legal person or arrangement.

  Records must be retained in an orderly manner that allows for effective analysis and the tracing of financial activities. They must be sufficient to reconstruct transactions in a manner that, if required, can support investigations or be used as evidence in legal proceedings. All CDD and transactional records must be readily available to Competent Authorities upon request and without undue delay.

1.4.1. DPMSR Reporting Requirements

DPMS are required to file a Dealers in Precious Metals & Stones Report (DPMSR) in the following circumstances:

- When conducting a transaction with resident individuals for cash equal to or more than AED 55,000 or its equivalent in foreign currency.
- When conducting a transaction with non-resident individuals for cash equal to or more than AED 55,000 or its equivalent in foreign currency.
- When conducting transactions with companies/entities equal to or more than AED 55,000 or its equivalent in foreign currency whether in cash or through wire transfer.

The obligation to file a DPMSR is not risk-dependent and must be fulfilled even when CDD measures have been satisfactorily completed and no red flags have been identified. Failure to submit a DPMSR within the predefined parameters and timelines may undermine the effectiveness of the entity's compliance framework and exposes it to enforcement action.

Entities must ensure that the process of filing a DPMSR is fully integrated into their operational workflows. This includes maintaining accurate records of transaction values, payment methods, parties involved, and relevant timelines to support accurate and timely reporting.

When entities are presented with a transaction that exceeds the DPMSR threshold and have reasonable grounds for suspicion, they must ensure that both, the threshold-based reporting and suspicions-based reporting obligations, are met in accordance with their respective requirements. Effective reporting relies on well-defined internal escalation mechanisms, clear allocation of responsibilities between business functions and the Compliance Officer, and ongoing staff training. Senior management remains responsible for ensuring that reporting obligations, whether it was based on a suspicious activity / transaction or threshold-based reporting, are understood, resourced, and embedded within the entity's overall AML/CFT/CPF compliance framework.

The ultimate purpose of all the above measures is to prevent the DPMS sector from being exploited for the purpose of ML/TF/PF by establishing effective mechanisms of identifying true beneficial ownership, tracing of movement of funds / assets and timely detection and reporting of suspicious activities to further support Competent Authorities in their efforts to detect, investigate and prevent financial crime.

The following sections of this Supplemental Guidance further expand on the obligations listed above and provide additional guidance specific to the sector.

2. Sector & Risk Context

2.1. Regulatory Definition of Precious Metals & Stones

While the definition of precious metals and stones may vary, somewhat depending on the region, the most generally accepted classifications internationally are based on factors such as quality, intrinsic value, and rarity. Accordingly, precious metals are said to consist of gold, silver, and platinum-group metals (platinum, palladium, iridium, osmium, rhodium and ruthenium). Precious stones are said to consist of diamonds, emeralds, rubies, and sapphire; while not technically gemstones, pearls are often also included in the category of precious stones and are thus included for the purpose of this Supplemental Guidance.

These generally accepted classifications are in line with the UAE's federal legislation which governs the control, stamping and identification of PMS, as well as the import and export requirements concerning raw diamonds under the internationally accepted Kimberley Process Certification Scheme (KPCS)[3]. Thus for the purpose of applying AML/CFT/CPF measures, the following definitions apply to PMS when determining applicability:

Precious Metals

- Gold, with a minimum purity of 500 parts per 1,000
- Silver, with a minimum purity of 800 parts per 1,000
- Platinum, with a minimum purity of 850 parts per 1,000
- Palladium, with a minimum purity of 500 parts per 1,000.

Precious Stones[4]

- Diamonds (rough), of any weight in carats
- Diamonds (polished), with a minimum weight of:
  - 0.3 carats per stone if loose, or
  - 0.5 carats per any single stone when mounted in a setting, whether of one or more stones
- Coloured gemstones, including polished emeralds, rubies and sapphires, with a minimum weight of:
  - 1 carat per stone if loose, or
  - 2 carats per any single stone when mounted in a setting, whether of one or more stones
- Coloured gemstones (polished Emeralds, Rubies, Sapphires), with a minimum weight of 1 carat per stone if loose, or a minimum weight of 2 carats per any single stone mounted in a setting (whether of one or more stones).

Pearls

- Loose pearls, with a minimum diameter of 3 millimetres per bead
- Pearls strung or mounted in a setting with a minimum diameter of 10 millimetres per any single bead, whether of one or more beads

Other Materials of Comparable ML, TF, PF Risks

Notwithstanding the above definitions, for the purpose of applying AML/CFT/CPF measures, DPMS should also consider PMS to include any object where at least 50 percent of its monetary value is derived from precious metals or precious stones, irrespective of its form or intended use.

Furthermore, DPMS should recognize that they may engage in transactions involving other types of metals and gemstones (whether traded regularly or occasionally, and whether physically or through electronic or virtual exchanges) which, while technically not considered to be PMS (despite being of high value in some cases), may nevertheless be subject to ML, TF and PF risks or other predicate offence risks (e.g. fraud) similar in nature to PMS. Such materials may include, but are not limited to:

- Other high-value metals used as part of DPMS activities, including platinum-group or platinoid metals (e.g. rhodium)
- Semi-precious gemstones (e.g. amethysts, opals, jade, and others)
- Synthetic, treated, or artificial gemstones (e.g. diamonds, emeralds, rubies, sapphires, pearls).

[3] See Federal Law No. (13) of 2004 on Controlling the Importation, Exportation and Transit of Raw Diamonds, as amended by Federal Law No. (4) of 2008.
[4] The weight thresholds define the point at which the precious stones typically acquire sufficient value and liquidity to pose material ML, TF and PF risks.

While this Supplemental Guidance focusses on the ML, TF and PF risks associated specifically with PMS, DPMS should also take a similar risk-based approach to the consistent application of AML/CFT/CPF measures in relation to covered transactions[5]. In doing so, DPMS should take into account the nature of transaction, customer behaviour and relevant risk indicators. Risk considerations should drive the application of AML/CFT/CPF measures and not solely rely on the technical classification of a product or the mechanical application of monetary thresholds.

2.2. Regulatory Designation of Dealers in Precious Metals & Stones

Under the AML/CFT/CPF Law and the AML/CFT/CPF Resolution, DPMS are obliged to apply the required AML/CFT/CPF measures when they qualify as DNFBPs. This obligation occurs where a DPMS carries out any single transaction, or series of transactions that appear to be related, whose monetary value equals or exceeds AED 55,000. This may include one or more transactions involving the same business relationship or customer, whether related to a single item or set of items; or it may also include one or more transactions which, in the judgment of the dealer, appear to be structured so as to avoid the established threshold. The nature of transaction, customer behaviour other relevant risk indicators should be considered when determining whether transactions are related or structured.

Some examples of when application of the AML/CFT/CPF measures is (or is not) required are provided below to illustrate how monetary threshold applies in practice[6]:

- A counterparty or a customer makes cash purchases of several different items at the same time, including a variety of PMS, whether loose or mounted, and requests separate invoices for each piece. No individual invoice meets the threshold of AED 55,000, however the total purchase price exceeds this amount. These are covered transactions.
- A counterparty or a customer wishes to purchase one or more items with a total value meeting or exceeding the AED 55,000 threshold and places a 25 percent deposit (below the threshold) in cash. A week later, he pays another 25 percent cash instalment, and after another week pays the remaining balance (which is below the threshold) in cash. The transactions are all related and are therefore covered transactions.
- Three customers enter a retail jewellery shop and together look at different set pieces. They each decide to buy diamond or gold jewellery worth AED 50,000, and all three wish to pay in cash on separate invoices. Although they are ostensibly different customers and each purchase is below the AED 55,000 threshold, the total amount is well over the threshold, and the customers are clearly associated. These are covered transactions.
- A gold trading company buys a consignment of gold bullion worth AED 375,000 from a wholesale merchant. The buyer places a deposit of AED 50,000 in cash and says that he will arrange for the balance to be paid along with the pickup of the bullion the next day. On the following day, a van arrives from a well-known local courier company to pick up the gold, and the driver delivers to the merchant a cashier's cheque for the balance of AED 325,000. Although the cash deposit was below the threshold, cashier's cheques (like money orders, treasury bills, bearer bonds, etc.) are negotiable bearer instruments and, as such, are cash equivalents. This is a covered transaction.
- A retail dealer accepts a diamond and emerald ring valued at AED 10,000 from a customer as a trade-in towards partial payment for the purchase of a diamond pendant worth AED 60,000, resulting in a net cash transfer of only AED 50,000. Although the cash portion of the payment is below the threshold level of AED 55,000, the payment in-kind in the form of the traded-in ring is a cash equivalent. This is a covered transaction.
- A dealer in gold bullion sells coins to a retail customer for a marked-up price of AED 56,000. The customer pays in cash. The coins' market value by weight on the international exchanges on the day of the sale is AED 49,000, and their book value is AED 49,500 based on the dealer's cost at the time he originally acquired the coins. This is a covered transaction. The DPMS's obligation to apply the AML/CFT/CPF measures is based on the fact that the actual price paid in cash exceeds AED 55,000, even though neither the coins' market value nor their book value meets the threshold.
- A diamond cutting and polishing firm wishes to buy a consignment of KPCS-certified rough diamonds from a local wholesaler. The two parties arrive at a final negotiated price of AED 950,000, which includes the payment being made in the form of a cash deposit of AED 50,000, with the balance being covered through several negotiable third-party promissory

[5] To clarify, the designation of a transaction as a covered transaction does not exempt the application of risk-based AML/CFT/CPF measures to transactions below the defined threshold where risk is present. Transactions that appear structured to avoid the threshold, or transactions which give rise to suspicion, remain subject to scrutiny and reporting obligations irrespective of value.
[6] These examples are non-exhaustive and should not be interpreted as limiting the circumstances in which transactions may be considered covered transactions under the AML/CFT/CPF Law and the AML/CFT/CPF Resolution.

notes from members of the Dubai Diamond Exchange and other internationally recognised diamond bourses (all belonging to the World Federation of Diamond Bourses). Although the cash deposit is less than the AED 55,000 threshold, the promissory notes are bearer negotiable instruments considered to be cash equivalents. This is a covered transaction.

- As part of his retail jewellery business, in addition to numerous rings, necklaces, bracelets and other set pieces, an established merchant normally sells only one or two loose diamonds, worth AED 2,500 to AED 3,500 each, in an average month. This pattern has been fairly stable for many years. This month, however, the merchant notices a marked increase in his sales of loose diamonds, which reach a level of 10 stones worth an average of AED 4,500 to 5,000 each, all of which are paid for in cash. The next month, sales of loose gemstones continue to increase, far beyond the normal pattern. Although each sale appears to involve a different customer, and they are all individually far below the AED 55,000 threshold, they are all in cash. Once the DPMS notices the sudden change in pattern and that total cash sales of loose diamonds have reached the AED 55,000 threshold, he should begin to apply the AML/CFT/CPF measures in order to assess whether these transactions may be related and thus be categorised as covered transactions.
- An art dealer sells a sculpture, more than two-thirds of whose value is comprised of 18K gold and fine (950) platinum, for AED 100,000 in cash. Although the intrinsic value by weight of the gold and platinum content of the statue is worth more than the AED 55,000 threshold, the art dealer is not obliged to apply the AML/CFT/CPF measures required of DPMS, since the sale of PMS does not make up a regular component of his business and he is therefore not considered to be a DPMS.
- The customer from the above example brings the sculpture he acquired to a DPMS a week later, and offers to sell it for AED 54,000, based on the content of the precious metals it contains, but he insists on being paid in cash. The dealer estimates the value of the gold and platinum he can obtain from melting down the statue to be approximately AED 70,000, before his costs. Although the amount of cash demanded is below the threshold of AED 55,000, this is a covered transaction. The DPMS should apply AML/CFT/CPF measures, based on both the value of the PMS content (which exceeds the threshold) and the appearance of structuring to avoid the AED 55,000 threshold.
- A retail jeweller brings 9 karat diamond studded jewellery for refining to a gold refinery and requests for diamond separation and gold refining. The value of the lot of jewellery is AED 90,000 and the charges from the refinery paid in cash by the retailer is AED 2500. This is a covered transaction even though the cash involved is below the threshold the exchange of the material in the form jewellery is above the threshold and hence is a covered transaction.

As long as DPMS carry out covered transactions, they are mandated to fulfil all of the AML/CFT/CPF programme obligations specified in the AML/CFT/CPF Resolution which include, but are not limited to, the preparation and implantation of AML/CFT/CPF policies and procedure, conducting business-wide and customer risk assessments, maintaining a defined AML/CFT/CPF governance framework, appointing a qualified Compliance Officer, implementing customer due diligence measures, conducting screening which is inclusive of politically exposed persons, reporting and monitoring cash transactions (where applicable), continuously monitoring transactions, reporting suspicious activities / transactions, maintaining records as per the regulatory obligation, adhering to Targeted Financial Sanctions (TFS) screening obligations.

It should also be noted that certain of the AML/CFT/CPF obligations under the AML/CFT/CPF Law and AML/CFT/CPF Resolution are independent of whether DPMS engage in covered transactions. For instance, DPMS are required to comply with instructions issued by the Competent Authorities of the UAE, concerning the implementation of United Nations Security Council Resolutions (UNSCR) adopted under Chapter VII of the UN Charter. It is important to note that while basic vigilance may be used for routine, low-value retail transactions which are remote from the threshold for covered transactions and do not pose any risk, in contrast, high-value and/or transactions close to the monetary threshold, repeated, structured or those that display attempts to avoid the application of such measures, should warrant for more than basic vigilance.

DPMS should always ensure that there is adequate allocation of resources and appropriate policies, procedures and systems are in place to enable the effective and timely application of all AML/CFT/CPF measures required.

2.3. Sector-Specific Risk Factors for Dealers in Precious Metals & Stones

The AML/CFT/CPF Resolution specifies certain risk factors that should be taken into consideration by DNFBPs when identifying and assessing ML/TF/PF risks at both the business and the customer levels.

General guidance on these risk factors is provided in *Section 8* of the *Guidelines for Designated Non-Financial Businesses and Professions*.

In addition to these generalised risk factors, there are several other which DPMS should be aware of and should take into consideration in identifying and assessing the ML/TF/PF risks to which they are exposed. Some of these risk factors depend on the specific stage of the PMS supply chain, and the role of the dealer in regard to the business relationships associated with each stage. These factors also relate to the nature and type of the customer or transaction involved. It is essential that DPMS identify the stage of the PMS supply chain they operate in to assess their exposure to ML/TF/PF risks in a manner that is commensurate with the nature, scale and complexity of their activities. This should include the consideration of UAE NRA and SRA outcomes.

Stages of PMS Supply Chain & Role of DPMS

The trade in PMS consists of a complex ecosystem or supply chain from extraction of the raw mineral to eventual sale to the final customer, in which numerous participants are involved. The risk involved in the upstream and downstream supply chains are different; heightened risks in regard to origin, traceability, smuggling and comingling tend to be associated with upstream activities whereas risks associated with placement, layering and integration of illicit proceeds tend to be associated with downstream activities. Thus, DPMS should take these distinctions into account when determining the level of scrutiny and controls to apply. The stages of the PMS supply chain are one where participants may conduct business with each other in multiple directions at different stages in the chain, and supply chain stages do not necessarily happen in order, and some stages may be skipped entirely. MoET expects DPMS to fully understand where they fit in the PMS supply chain and the risks associated to be able to tailor and deploy effective mitigating controls.

For the purpose of convenience, the various PMS supply chain stages, and some of the major ML/TF/PF risks to which each stage is vulnerable to, is simplified as follows:

Extraction/Production

In this stage, the raw minerals containing the PMS are extracted, whether through mechanised industrial means (as in underground or open pit mining) or through artisanal and small-scale methods (as in alluvial manual collection). This stage may also include the sorting and grading of raw minerals, extraction of metal for its ore by rudimentary methods or sophisticated technologies and their preparation for sale.

Key ML/TF/PF risks at this stage include, but are not limited to, the infiltration of the extraction/production process by criminal or terrorist organisations, vulnerability of the supply chain to the introduction of illicit PMS, or commingling, over/under invoicing or false invoicing and accounting fraud. This stage is also vulnerable to numerous predicate offences, such as theft, embezzlement, smuggling, and bribery/corruption. Thus, the extraction/production process may be used as a vehicle for both the creation of and the laundering of illicit proceeds.

Exposure to this stage of the supply chain calls for stronger emphasis on source of origin information, counterparty assessment and any indicators of commingling or illicit sourcing.

Trading in Raw Minerals

In this stage, raw ores, unrefined metal or rough gemstones are obtained from the extraction source and traded by dealers or intermediaries. This stage of the supply chain may also involve the export and import of raw ores, unrefined metal or rough gemstones. Moreover, the market for different types of raw PMS may have different characteristics and regulatory regimes. For example, the trade in rough diamonds is strongly impacted by the requirements of the Kimberley Process Certification Scheme (KPCS), as well as the fact that a significant portion of the international trade is conducted through a group of regulated bourses. DPMS may participate in this stage of the supply chain as traders of raw materials, either as importers, exporters, or as wholesalers or intermediaries in transactions between other physical or legal persons. Such transactions may take place on a direct party to counterparty basis, through tenders or auctions, or via electronic or internet exchanges.

This stage of the PMS supply chain can be one of the most vulnerable to ML/TF/PF risks, in that the number and variety of participants (including street vendors, aggregators, exporters and regional dealers) can be high, and raw minerals may pass through numerous traders' hands before moving on to the next stage of the supply chain. Moreover, in the case of some categories of PMS, operational, accounting, and fiscal controls can often be decentralised over multiple geographic regions and legal jurisdictions, making them vulnerable to exploitation by fraudsters, criminals, and terrorists.

Key ML/TF/PF risks include but are not limited to commingling or entry of conflict minerals into the supply chain, benefitting criminal or terrorist organisations (through falsification of Kimberley Process certifications, in the case of rough diamonds, or smuggling and illegal placing into the market of products from non-participating countries; and due to the absence of international controls equivalent to the KPCS in the case of other PMS, commingling of metal from conflict affected and high risk areas with lower risk jurisdictions to falsify the origin, wrong declaration of value, weight or purity of the metal to evade taxes, royalty or duties). Infiltration of criminal or terrorist organisations among raw mineral traders, prevalence of cash (or cash equivalent) transactions and vulnerability to smuggling are among the ML/TF/PF risks.

This stage of the PMS supply chain warrants enhanced scrutiny of counterparties, payment methods, and trade documentation especially where there is involvement of multiple intermediaries or cross-border movements.

Beneficiation

In this stage of the PMS supply chain, raw minerals are transferred to technically specialised intermediaries for purification and preparation for sale by various processes, such as refining/smelting in regard to precious metal, and cutting and polishing with respect to precious stones. This stage can also include the recycling of existing PMS (e.g., the re-smelting of scrap precious metals, or the re-cutting and polishing of precious stones). DPMS may participate in this stage of the supply chain as technical specialists (refiners, cutters, polishers, etc.), or as wholesalers, agents, buyers or sellers trading with, or on behalf of, such specialists.

Key ML/TF/PF risks at this stage include, but are not limited to, the obscuring of traceability of PMS through the beneficiation process, trade-based ML (TBML), the prevalence of cash/cash equivalent transactions, and vulnerability to commingling. This stage is also vulnerable as tracing of the origin of the PMS is very difficult once it goes through the beneficiation process.

DPMS in this stage of the PMS supply chain should ensure the deployment of adequate controls especially relating to the source of origin information and consistency of purity, volumes and valuation.

Wholesale Trade

In this stage, processed PMS (either refined precious metals or cut and polished precious stones), as well as finished goods (i.e. jewellery) are traded on a wholesale basis for a variety of purposes, and through diverse channels, some of which may entail the physical exchange of goods and others of which may be virtual in nature (for example, through certificates or various derivative products). These purposes may include but are not limited to transactions involving:

- Sales to manufacturers/fabricators (e.g. jewellers, factories) for use in various finished products or industrial processes
- Sales to/from other wholesaler dealers/intermediaries or retail merchants for inventory, stockpiling, or speculation/trading
- Sales related to FIs or commodity exchanges for trading or investment purposes

DPMS may participate in this stage of the supply chain as wholesale traders or intermediaries, as well as agents/buyers/sellers on behalf of industrial and retail end users.

Key ML/TF/PF risks at this stage include but are not limited to commingling, trade-based ML, and other known typologies and methods associated with placement, layering and integration.

It is imperative that DPMS in this stage have sufficient awareness and capability to spot out and mitigate risks related to various trade-based ML typologies, complex transactional structures and the use of intermediaries or third-party payments. DPMS handling bullion or scrap must evidence origin plausibility, reconcile weight/purity vs documentation and treat unverifiable 'scrap' claims as high-risk.

Retail Trade

In this stage, beneficiated PMS or finished goods (jewellery fabricated from PMS) are sold to, or acquired from, retail customers in the primary or secondary markets. DPMS involved in this stage are usually retail merchants involved in selling or buying direct to/from the public. This stage is particularly vulnerable to ML/TF/PF risks connected with commingling, as well as to the classic ML/TF/PF risks associated with placement, layering and integration, and to predicate offences such as fraud, theft and robbery or embezzlement, among others.

This stage of the PMS supply chain warrants for greater emphasis on monitoring customer behaviour, transaction patterns, payments methods especially where high-value or repeated transactions occur.

Supply Chain Stages and Roles of DPMS[7]

There are many different stages and transactions and counterparties involved in the precious stones and precious metals businesses. As set forth above, miners range from international companies to individuals. Intermediaries may be well established local buyers from miners, or itinerant foreign buyers, or hawalas. Retail jewellers may buy articles of used jewellery, as may direct buyers and pawnshops. Each of these businesses may present a money laundering risk. Dealers may buy from or sell to other counterparties who also work in their precious metals or precious stones businesses or sell to the public through retail sales (which may often be anonymous). Dealers will need to consider the risks associated with each stage at which they participate. A risk-based approach should account for higher risk customers and counterparties at every stage.

Apart from the retail sector, trade in diamonds, jewels and precious metals is traditionally private, as a matter of commercial protection or security. Dealers have traditionally protected their counterparties, their materials, and their business practices from public knowledge, in the interest of protecting themselves from criminal activity, and from potential independent interaction by competitors with their customers and counterparties or suppliers. However, it is necessary for dealers themselves to know that they are dealing with legitimate counterparties.

In some sectors within precious metals and precious stones businesses, trust based on personal contact is an essential element of conducting business, and such trust and personal contact assist in lowering counterparty risk. In addition, each industry has trade resources, such as trade associations and directories, with which to establish some background and credit information and these should be consulted. Checks must be made upon any new counterparty that is unknown to a dealer, and particularly if also unknown within the dealer's industry. A counterparty, who proposes a transaction in diamonds, jewels or precious metals should have the knowledge, experience and capacity, financial and technical, to engage in that transaction.

Nature and Type of Counterparty/Customer, Product/Service or Transaction

When required to apply AML/CFT/CPF measures, DPMS acting in any of the roles / stages mentioned above should carefully consider risk factors in relation to customers, geographic exposure, channel, product / service and transaction type (*Section 8* of the *Guidelines for Designated Non-Financial Businesses and Professions*). The following risk factors, in combination and together with any other relevant factors, support DPMS in developing an overall risk profile which will essentially determine the level of scrutiny and risk mitigation measures required. It is important to note that the presence of one or more high-risk factor does not automatically indicate ML/TF/PF risk, rather it warrants enhanced diligence and additional risk mitigation measures on the basis of the overall risk profile derived. Furthermore, the following factors are not exhaustive and should be taken into account together with other relevant risk factors in order to form an overall risk profile that informs the risk mitigating framework.

- Customer / counterparty type, complexity and transparency (e.g. whether the counterparty or customer is a physical person, a legal person or a legal arrangement; if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a PEP)—particularly in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level in regard to the product or service and transaction type is appropriate
- Country of origin of the PMS, particularly in relation to whether the country is a known production or trading hub for the type of PMS; has adequate regulations and controls (for example, is a participant in the KPCS for rough diamonds); is a High-Risk Country (e.g. is subject to international financial sanctions, part of the FATF black or grey-lists has a poor transparency or corruption index, is a known location for the operation of criminal or terrorist organisations), or is the location identified as a hub which transits a lot of PMS from conflict affected and high risk areas
- Country of origin or residence status of the counterparty or customer (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country) particularly in relation to the locations where the transaction is conducted and the goods are delivered

[7] Refer RBA Guidance for Dealers in Precious Metal and Stones, FATF/OECD, June 2018, p. 22.

Note: Entities are strongly encouraged to develop their own country-risk model that takes into consideration publications issued by the NAMLCFTC, analytical reports and advisories issued by the UAE FIU, the FATF lists of High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring, as well as the OECD list of jurisdictions classified as uncooperative tax havens. The country-risk model should be documented, applied consistently across customers and suppliers, and subject to periodic review to ensure continued relevance in light of evolving ML/TF/PF risk exposure.

- Channel by which the counterparty/customer is introduced (e.g. referrals versus walk-in, international versus domestic, in-person or via the internet or other media) and communicates (e.g. remote or personal contact, direct or indirect through a proxy)
- Type, nature and characteristics of the products and/or services, including but not limited to quantity, quality/level of purity, price/value, form (whether physical or virtual, raw/rough or processed/finished, etc.), rarity, portability, potential for anonymity
- Type, size, complexity, cost and transparency of both the transaction (including whether the physical or virtual exchange of merchandise is involved) and the means of payment or financing—particularly in relation to whether they appear to be consistent with the counterparty or customer's socio-economic profile, local market practices, and the degree of expertise required
- Novelty or unusual nature of the transaction or financial arrangements (including, for example, requirements to expedite the transaction beyond what is customary, unusual delivery requirements, or unusual requests for secrecy), particularly compared with what is normal practice in the local market.

Geographic Risk[8]

Geographic risk is pivotal, particularly at upstream supply chain stages – more specifically, in relation to mining and initial sourcing operations. Mining can be vulnerable to terrorist financing if it occurs in remote locations with minimal governmental presence or infrastructure. In some areas, for example, gold mining can be dominated by armed non-governmental groups. Mining for jewels is also geographically widespread and sometimes occurs in areas of significant turmoil. Unlike diamond mining, mining for jewels is largely small and informal, carried on by local prospectors and owners in alluvial sources, very few of which, if any, are publicly traded companies. Some mines are government owned, and mines often have licenses issued by government agencies involved with natural resources, but even such mines are often remote from strong governmental oversight, and often in areas of substantial conflict and crime, including terrorism. Buyers travel to the mines or to nearby communities and buy jewels, sometimes in a manner controlled by government, sometimes either directly from miners or from local intermediaries. Because many of these areas do not have reliable financial systems, payments are often in cash and informal, or are made through third party accounts, increasing risk.

Thus, a customer who is a UAE national seeking, in person, to purchase a modestly priced diamond engagement ring may have a very different ML/FT risk profile from that of a foreign national seeking, via remote communication (such as telephone or email), to purchase gold bullion using bearer negotiable gold certificates, or loose polished diamonds for delivery to a location in a third country. A combination of risk factors arising from customer characteristics, product types, geographic exposure, delivery channels and payment methods contribute to such differences, which should be considered holistically when assessing risk. The types of risk profiles identified and assessed, and the resultant risk ratings applied to the customers, should be used in determining the efficient allocation of AML/CFT/CPF resources, as well as the appropriate application of reasonable and proportionate risk-mitigation measures, including customer due-diligence measures (discussed below).

In assessing ML/TF/PF risks and assigning risk ratings to their customers, DPMS may utilise a variety of methods, depending on the nature and size of their businesses. These may include more sophisticated models, such as the application of risk weightings to the various risk factors identified, and the calculation of an overall risk score for each customer; or simpler methods such as the development of indicative customer ML/TF/PF risk profiles based on their business models, standard market practices, and target customer segments, against which customers may be filtered and risk-rated. The methodology adopted should be proportionate to the nature, scale and risk exposure of the DPMS's activities. Furthermore, whichever method is chosen, DPMS should clearly document them (including the rationale for their use), and apply them consistently across their business

[8] Refer *RBA Guidance for Dealers in Precious Metal and Stones*, op. cit., p. 21.

activities. Periodic review and, where appropriate, update of methodologies is mandated to ensure relevance in light of changes in the risk and regulatory landscape as well as changes to the nature of business activities, strategies or objectives.

3. Due Diligence and Ongoing Monitoring

Together with the accurate identification and assessment of ML/TF/PF risks and the ongoing monitoring of customer relationships and transactions, the implementation of reasonable and proportionate customer due-diligence measures is one of the key components of an effective risk-based AML/CFT/CPF programme. The *Guidelines for Designated Non-Financial Businesses and Professions*, of which this supplemental guidance is a part, discusses customer due diligence (including enhanced and simplified customer due diligence measures) in detail, and DNFBPs should refer to the related sections of the Guidelines carefully and comply in full with CDD/EDD, monitoring, sanctions screening and record-keeping requirements. Nevertheless, there are some additional points that are of particular relevance to DPMS. These additional points highlight typologies and risk indicators specific to the DPMS sector which are intended to support entities in implementing measures in a manner that is risk-based, proportionate and effective.

First, irrespective of the size of the transaction or the method of payment, DPMS should ensure that they have in place a process for screening existing and prospective business relationships and customers against Sanctions Lists, and for performing background checks on them to identify any potentially adverse information (including associations with PEPs, or financial or other crimes. In this regard, DPMS should become familiar with the various tools available for these purposes, including but not limited to publicly accessible government and intergovernmental Sanctions Lists; commercially available or subscription-based customer intelligence databases and due-diligence investigation services; and the use of internet search techniques. It must be noted that DPMS are expected to ensure that the depth and frequency of screening is commensurate with the associated risks.

Second, a characteristic technique used in a variety of ML/TF/PF typologies is the attempt to conceal beneficial ownership through the use of third-party intermediaries, proxies, or legal structures or arrangements, which can help to create distance between the source of the illicit funds and the transaction or activity in question. Such third-party intermediaries may include family members, friends, business associates, other legal representatives, or other third persons. In this regard, when carrying out covered transactions, DPMS should be particularly attentive to establishing and verifying the identity of the true beneficial owner and, considering the risk involved, corroborating the legitimacy of their source of funds through reliable independent sources, wherever ongoing business relationships are concerned, or when high risk situations are identified involving occasional or one-off customer transactions.

Typically, the starting point in determining beneficial ownership of a legal entity or legal arrangement is to ask pertinent questions and to obtain information directly from the business relationship or customer. The information thus obtained should be analysed for reasonableness and consistency and should be appropriately confirmed or corroborated with reference to reliable independent sources whenever possible, using a risk-based approach (for example, when higher risk situations are identified). Thus, sole reliance on representations provided by customers where the overall risk profile warrants enhanced scrutiny. This verification process may raise additional questions that require further scrutiny by the DPMS and clarifying explanations from the business relationship or customer, with the goal of ensuring reasonable satisfaction that the DPMS knows the identity of the true beneficial owners and believes their source of funds to be legitimate.

Generally, in the context of this corroboration process, reliable independent sources may include (but are not limited to) such things as bank references or bank account information provided by financial institutions or commercial credit reporting agencies/services; the use of public registries and/or tax information, such as commercial registries or federal/national tax identification numbers to verify the ownership of legal entities. In cases where such sources are unavailable, DPMS should consider reliable alternatives as means of corroboration, ones that are appropriate to the level of risk identified. When required to conduct customer due diligence, DPMS should be alert to situations in which existing or prospective business partners or customers appear unable or unwilling to divulge relevant ownership information or to grant any required permissions to third parties to divulge such information about them for corroboration or verification purposes. Heightened risk could be indicated through such circumstances which are contextual.

They should also be alert to customer due-diligence factors such as:

- Compatibility of the customer's profile (including their economic or financial resources, and their personal or professional circumstances) with the specifics (including nature, size, frequency) of the transaction or activities involved.
- Utilisation of complex or opaque legal structures or arrangements (such as trusts, foundations, personal investment companies, investment funds, or offshore companies), which may tend to conceal the identity of the true beneficial owner or source of funds;
- Possible association with politically exposed persons (PEPs), especially in regard to foreign customers.

The aforementioned factors should be taken into account at the time of establishing a business relationship as well as during the course of the relationship (on an ongoing basis). The application of due diligence measures should be informed by the risk assessment undertaken, including the intensity of ongoing monitoring. DPMS must refuse or exit relationships where beneficial ownership or source of funds/origin cannot be reasonably verified or where sanctions/PF risks cannot be mitigated.

3.1. Ongoing Monitoring

Under some circumstances (for example, in the case of ongoing business relationships with suppliers or customers), DPMS may be in a position to monitor the status and activity of the business relationship over time. However, in other situations (such as those involving occasional or one-off customer transactions, or retail sales), it may not always be possible for DPMS to perform detailed ongoing monitoring of the entirety of their business partners' or customers' activity. Nevertheless, it is important that DPMS take reasonable steps to protect themselves from misuse by criminals and terrorists. Particularly in circumstances in which high-risk customers have been identified, DPMS should make reasonable efforts to monitor activity related to the transactions, services, or customer activities with which they are involved. Some examples of ways in which they may do so include, but are not limited to:

- In cases of covered transactions: Maintaining careful records of the certificate numbers and/or identifying characteristics (including weight, purity/quality, colour, shape, cut, inclusions or other markings, and other relevant factors) of the PMS involved.
- In cases of warehousing or safekeeping of PMS on behalf of business partners or customers: Maintaining careful records (see above point) and monitoring the status of the merchandise throughout the course of the transaction or account life cycle, in order to detect any unusual changes or substitutions.
- In cases of performing contracted services (such as refining, cutting or polishing, or selling on consignment or memorandum): When collecting fees for their services, ensuring that the funds received come from known sources on which they have performed CDD, and not from third-parties, foreign accounts, or other unknown sources.

In general, ensuring whenever possible that the methods of payment and/or the financial instruments used are consistent with the customer's profile, and are not methods which could disguise the origin of the funds (such as cash, cashier's cheques, traveller's cheques, postal money orders, prepaid cards, third-party endorsed cheques, cryptocurrencies, IOUs, promissory notes or other difficult-to-trace payment methods); and when it is necessary to accept such forms of payment (especially cash), recording as much information as possible, such as the denomination and serial numbers of the banknotes or complete details regarding negotiable instruments.

The above examples are intended to serve as practical monitoring measures relevant to the various DPMS business models and stages of the PMS supply chain. The implementation of monitoring measures should be proportionate and risk-based and where anomalies are identified through monitoring, the associated risks should be assessed and subject to enhanced scrutiny and reporting where applicable.

4. Common Sectoral Challenges & Best Practices

4.1. Sectoral Challenges

- There is high fragmentation when it comes to the PMS supply chain, often involving multiple actors (miners, middlemen, refiners, wholesalers, retailers). This involvement of multiple small intermediaries, often across borders, brings about commingling risk. At each stage of the supply chain, material is prone to change hands multiple times and criminals exploit this complexity as once metal is re-melted or stones are re-cut and polished, origin becomes opaque as the PMS loses all trace of origin. This allows stolen gold or smuggled minerals to be placed into legitimate supply chains, enabling commingling and re-documentation. Conflict-affected or high-risk area gold can then enter markets through "clean" jurisdictions.

- The product characteristic of PMS is marked by high value in very small quantities, and this is alluring to criminals as these items can easily be moved across borders without drawing too much attention, relative to the movement of high value funds through the financial system. PMS can be stored discreetly and sold for cash or exchanged for other assets with relative ease and anonymity. These attributes create an alluring mechanism for storing and transporting criminal proceeds, especially from drug trafficking, corruption, fraud and tax crimes. It allows for the settlement of debts and potential funding of illicit networks, outside of formal channels.
- In many parts of the PMS sector, cash is still a dominant payment method bringing about challenges related to traceability. The ability to use cash equivalents provides criminals with a way to mimic legitimate payments whilst avoiding scrutiny and the ability to structure payments allows criminals to stay below reporting triggers.
- While comprehensive responsible sourcing programs have been implemented among refiners and large traders, minimal documentary verification, limited access to international certification schemes and reliance on trust-based or relationship-driven supplier arrangements poses challenges. Inability to validate mine-of-origin claims, insufficient translation or authentication of foreign documents, inadequate review of transport routes, shipping anomalies or changes in declared origin result in entry of conflict gold, stolen or illegally mined PMS or abuse by front companies masking sanctioned networks.
- The frequent involvement of cross-border shipments, third-party payments, multiple layers of invoices create fertile ground for trade-based money laundering with criminals often engaging in over/under-invoicing to shift value internationally , duplicate or create fake invoices to justify funds movement, use of multiple intermediaries to obscure buyer/seller identity, trans-ship through jurisdictions with minimal oversight, divergence between shipping routes, invoices and payment flows. These techniques can easily be deployed by criminals given that fact that gold and diamonds are difficult to value objectively without specialised expertise, minor manipulations in purity or weigh can justify large price variations and market volatility enables artificially inflated or deflated pricing.
- Organized networks increasingly infiltrate or mimic the DPMS sector through the use of shell companies, brokers operating without licences, nominee directorship or complex ownership structures to exploit the operational and structural environment of the sector such as ease of justifying large-value transactions, industry norms of informality and relationship-based trust, gaps in verification of beneficial ownership.
- SMEs with limited compliance staff, low training penetration, reliance on manual processes, limited ability to implement risk-based monitoring, difficulty interpreting regulatory mandates often lead to inconsistent identification of red-flags, inability to detect structured or patterned activity, under-reporting of suspicious transactions. Thus, low AML/CFT/CPF awareness, particularly among smaller DPMS, poses great challenges as lack of appropriate controls by entities allows criminals to easily infiltrate the sector.

4.2. Best Practices

- DPMS should demonstrate national, sectoral and business level risk awareness and implement a documented and proportionate risk-based approach to mitigating ML/TF/PF risks. The risk-based approach deployed must guide all aspects of compliance from customer onboarding to monitoring and escalation. This requires undertaking periodic risk assessments covering key risk factors across customer types, supply chain exposure, jurisdiction risks, delivery channels, product types and payment channels. Structured methodologies should guide risk scoring, weights of risk factors and qualitative assessment, consistent with the scale and complexity of activities. Senior management approval and involvement in the risk-based approach process remain pivotal. Risk assessment must be subject to routine updates, especially where significant changes occur in business, risk or regulatory environments.
- Entities must establish a strong governance structure appropriate to the size of their business and risk exposure. A qualified AML/CFT/CPF Compliance Officer / Money Laundering Reporting Officer (CO/MLRO) with sector-specific knowledge and sound understanding of regulatory obligations must be appointed. Independent testing or audit of AML/CFT/CPF programmes should be implemented. There should be written policies and procedures aligned with regulatory mandates and best practices. All employees must undergo regular AML/CFT/CPF training, including front-line staff and senior management. Entities must ensure group-wide AML/CFT/CPF frameworks where there are multiple branches or affiliates.
- Due diligence remains critical to preventing sector misuse for ML/TF/PF. Entities must understand who they are dealing with, the purpose of business relationship and transaction and whether associated activities are consisted with a legitimate profile. Thus, verification

of identity through reliable and independent sources. Identifying beneficial owners of legal persons or arrangement, understanding ownership/control structures, determining the intended nature and purpose of business relationship / transactions is at the core of customer due diligence measure applied. Where there is association with high-risk jurisdictions, politically exposed persons and close associates, customers using cash or cash equivalents as primary funding instruments, non-resident customers or intermediaries where the role is unclear and there is no economic rationale should warrant for enhanced due diligence. Furthermore, entities must implement ongoing monitoring that is proportionate to the customer risk.

- Given the elevated global risks associated with the trade of PMS, especially in upstream phases related to PMS sourcing and in jurisdictions with weak governance, entities should identify all counterparts in the PMS supply chain. assess the risk level of all suppliers involved, verify origin pf gold, rough diamonds and other PMS using export certificates (KPCS for rough diamonds), customs declarations and shipment documents. Entities must compare declared origin to known production capabilities of the jurisdiction. Where documentation is incomplete, inconsistent or unverifiable, shipments are to be rejected. Intermediaries should be carefully managed, mandating justification for involvement and clear linkages to the customer and transactions. There should be enhanced scrutiny where there are goods that transit through high-risk jurisdictions.
- Entities must scrutinize price deviations from global benchmarks, check for mismatched weights, purity or discrepancies in documents, detect circular trading patterns, review and identify trade routes for unusual detours or shipments to jurisdictions know for weak oversight and validate third-party payments whilst ensuring plausible economic rationale. These measures help deter trade-based money laundering as the sector is highly exposed due to the cross-border nature of its trade activity.
- DPMS must align their AML/CFT/CPF measures with lists of high-risk and monitored jurisdictions. All customers and suppliers must be mandatorily screened against the UNSC and UAE Terrorist Lists. FAFT listed countries should be taken into account when undertaking risk assessments, particularly related to demography/jurisdictions risk. Where associations to jurisdictions subject to increased monitoring are identified, enhanced due diligence and enhanced monitoring must be undertaken.
- Clear and documented internal escalation procedures must be put in place and employees must be trained to identify red flags to TBML schemes, third-party involvement, structuring, PF and sanctions evasion techniques and all other sector typologies. Suspicious activity / transaction reports as well as threshold-based reports must be promptly filed with relevant authorities whilst maintaining confidentiality of internal and external reporting processes.

5. Typologies

As mentioned in the Guidelines, the methods used by criminals for money laundering, the financing of terrorism, and the financing of illegal organisations are continually evolving and becoming more sophisticated. Moreover, the variety of transaction and activity types involving DPMS can be very wide. It is therefore impossible to provide an exhaustive list of ML/TF/PF typologies for DPMS, as new typologies and techniques are constantly being developed and attempted.

Nevertheless, research on the subject and analysis of case studies from around the world have identified some common methods used by criminals for the purposes of ML/TF/PF involving DPMS. These methods broadly align with the classical stages of the ML/FT process (i.e. placement, layering, and integration; however, they can also involve PMS as a vehicle for committing a predicate offence, or as the direct proceeds of crime.

DPMS should recognise that, often, multiple ML/FT typologies and techniques are used in a single transaction or in a series of related transactions. They should therefore be alert to indicators of potentially suspicious transactions from all categories. Furthermore, they should be sure to incorporate the regular review of ML/TF/PF trends and typologies into their employment screening and compliance training programmes as well as into their risk identification and assessment procedures.

The following have been identified as being amongst the common typologies used for exploiting DPMS for the purpose of ML/TF/PF, according to the Financial Action Task Force (FATF)[9]:

[9] See, for example, *Money Laundering and Terrorist Financing through Trade in Diamonds,* op. cit.*; Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold,* op. cit.*; and Professional Money Laundering,* op. cit.

Use of PMS as an alternative to currency

Due to their specific characteristics, PMS (and diamonds and gold, in particular) can be an attractive means to store value. This status can lend itself to utilisation of PMS by criminals as an alternative form of payment for illicit goods and services, which can be smuggled relatively easily and later converted to cash or other traditional and non-traditional forms of value or value transfer, bypassing the formal financial sector and its associated controls. Analysis of case studies has shown a correlation between the use of diamonds and gold as currency and drug trafficking; however, it has also been reported in cases related to other categories of crime, such as illegal arms dealing, human trafficking, environmental crimes, and others[10].

PMS as stored value instruments/means to realise the proceeds of crime

PMS (and diamonds and gold, in particular) are an international commodity, easily traded, transferrable across borders, and able to retain (or even appreciate in) value over relatively long periods of time. These characteristics, along with their relative anonymity, and even their ability to be insured, warehoused, and changed into different physical forms, make them well-suited to serve as a means of longer-term value storage and ML.

When it comes to PF/sanctions evasion, the risk can emanate from efforts to transfer value into high-value PMS for subsequent transport or sale, frequently demonstrating weak association between the customer's profile and the scale/purpose of the underlying transactions.

Laundering illegal PMS and/or the use of PMS to launder the proceeds of crime

As noted in parts of this guidance, the PMS supply chain is complex and can involve multiple participants in each stage, with varying levels of control and numerous vulnerabilities to ML/TF and associated predicate offences. Criminals may utilise a variety of techniques to realise value from illegal PMS, or to conceal, disguise, and/or transfer the proceeds of crime by utilising financial flows associated with the trade in PMS, at different stages of the supply chain. Such techniques may include but are not limited to theft or embezzlement; smuggling; commingling of illicit and legal materials; forgery or fraudulent certification; transfer pricing; misrepresentation of quantity, quality, or type of PMS; and many others. These techniques are often used when laundering the proceeds of crime through wholesale or retail DPMS.

Trade-based money laundering (TBML)

Due to the global nature of the trade in PMS, criminals may exploit opportunities to utilise this typology through PMS-related transactions and related financial flows. Some of the techniques employed include but are not limited to: over-invoicing, under-invoicing, or fraudulent invoicing, customs/VAT fraud, forgery and falsification of documentation, virtual trading, and others. These techniques are often associated with the use of major trading hubs for PMS, including free trade zones[11].

Additionally, PF-related networks, inclusive of efforts aimed at evading sanctions, tend to utilize trade strategies that intersect with trade-based money laundering typologies including inaccurate end-user declarations, routing across various jurisdictions or conflicting shipping agreements.

Repeated requests for proforma invoices, frequent document revisions or settlement without physical movement should be treated as high-risk TBML indicators and escalated.

Physical smuggling of PMS

Due to their high value-to-weight ratio, and other characteristics of PMS that make them difficult to detect or trace, they can be smuggled fairly easily. This is often done in conjunction with the other ML/TF methods referred to above, and may involve a number of different techniques, including the disguising of certain types of PMS as common low-value objects.

---

[10] See, for example, *Strengthening the Security and Integrity of the Precious Metals Supply Chain*, United Nations Interregional Crime and Justice Research Institute (UNICRI), May 2016.
[11] See, for example, *Money Laundering and Terrorist Financing through Trade in Diamonds,* op. cit., and *Money Laundering Vulnerabilities of Free Trade Zones*, FATF/OECD, March 2010.

Use of intermediaries and/or front/shell entities

In order to create layers of separation between sanctioned individuals / entities from transactions and/or business activities, PF and sanctions-evasion schemes sometimes rely on layered intermediaries and front companies. In a DPMS setting, this may appear as a legitimate trading relationship where the counterparty's ownership, controlling party, authorised signatories are ambiguous, subject frequent changes or are inconsistent with the declared profile. Such structures, often coupled with non-transparent trade documentation are common strategies aimed at evading sanctions and are recognized as patterns of DPMS abuse.

Exploitation of high-risk subsectors

DPMS subsectors, specifically bullion traders and refiners present elevated risks emanating from the elimination of origin identifiers through refining, re-melting or re-casting. This creates a layer of complexity in supply chain due diligence and where controls are inadequate, it enables commingling.

Bullion and refinery operations present elevated risks as refining, re-melting, or re-casting may eliminate origin identifiers and enable commingling when sourcing controls are inadequate. Exposure to PF/sanctions-evasion could occur if incoming materials come from, pass through, or are organized by entities linked to high-risk regions, where evidence of responsible sourcing is lacking, or where the chain of custody is ambiguous (including multiple ownership changes within brief periods). This classification is especially significant in situations where the customer is reluctant to furnish origin documentation, or when the economic justification for the supply chain is inadequate. The UAEFIU report highlights ongoing weaknesses in responsible sourcing and the necessity for enhanced controls across the sector

6. Red Flag Indicators

The following list of red-flag indicators for potentially suspicious activity / transactions is not exhaustive. It is important to note that the presence of one or more of these indicators does not automatically imply that a transaction involves a crime. Rather, it serves as an indication that enhanced due diligence, or further investigation may be warranted. The appointed Compliance Officer of the entity should carefully assess the circumstances to determine whether the activity / transaction is indeed suspicious.

6.1. Customer Behaviour

Structuring

- Customers intentionally structuring amounts to avoid identification or reporting thresholds. For example, numerous small transactions over a short period, such that each is below the regulatory threshold for the relevant level of customer due diligence (CDD), but the cumulative total is substantial. This behaviour is also known as Smurfing.
- A customer who approaches different branches of the same DPMS in a short period to conduct transactions below the reporting threshold.
- Repeated structuring behaviour observed over time, even where individual transactions appear compliant when viewed individually, indicating a pattern that may warrant enhanced review or further assessment rather than isolated or one-off activity.
- Customers who restructure transactions or split payments shortly after being informed of applicable reporting, record-keeping, or identification requirements, which may indicate an attempt to remain below regulatory thresholds and therefore require additional scrutiny.
- A group of individuals (especially non-residents) approaching the same DPMS, conducting multiple cash transactions below the reporting threshold.

Unusual Requests & High-Risk or Criminal Association

- Sudden and unusual inquiries about refund policies, followed by requests for large refunds.
- Requests to alter or cancel a transaction after being asked for identity or supporting documents.
- A customer exhibits an unusual hurry to complete the transaction.
- Abnormal requests for precious metal conversions into ordinary objects to disguise the identification of PMS.
- Sudden unexplained changes in the volume or value of transactions that are inconsistent with the customer's known profile.
- The customer appears related to a high-risk country, territory, or entity associated with CAHRA origin gold trading linked to money laundering or terrorism activities, or to a person designated as a terrorist.

- Potential involvement of shell companies, a parent or subsidiary of an offshore company, where the Ultimate Beneficial Owner (UBO) is difficult or impossible to identify.
- The customer is linked to negative news or criminal activities, such as being named in a news report about a crime or being under investigation by law enforcement.
- A politically exposed person (PEP) who is linked to negative news or crime, or any family member or close associate of such a PEP.
- A customer who is linked to a designated terrorist individual or organization.

Lack of Transparency or Documentation and Forgery

- The customer fails to provide sufficient explanation or documentation for the source of funds. For example, attempts to use a third-party cheque or credit card with questionable or untraceable ownership.
- The customer is unable or unwilling to provide information for due diligence and record-keeping purposes.
- Vague or refusal to provide information on the reason for buying or selling PMS, or about the origin of the items.
- The customer is unable or unwilling to identify beneficial owners or controlling interests, where this would be commercially expected.
- The customer is suspected of using forged, fraudulent, false, or digitally manipulated identity documents for due diligence and record-keeping purposes.
- Repeated requests to modify transaction terms, documentation, or counterpart details after initial compliance review.

Secrecy and Evasion

- The customer attempts to maintain a high degree of secrecy regarding the transaction, for example:
  - Requests that normal business records not be kept.
  - Refuses to provide information for due diligence and record-keeping purposes.
- The customer is unusually concerned with reporting thresholds or the Anti-Money Laundering (AML) / Combating the Financing of Terrorism (CFT) / Counter Proliferation Financing (CPF) policies of the entity.
- Frequent changes in ownership, management, or business names without a clear business rationale.
- Customer demonstrates heightened concern about FIU reporting thresholds or internal escalation processes.

Other Behavioural Red Flags

- The customer is accompanied by others who appear suspicious, such as lurking outside the premises or closely monitoring the customer and are evasive when asked for further details.
- The customer is employed by a DPMS entity but is conducting transactions in a personal capacity.
- The customer unnecessarily self-discloses that their funds are clean and not involved in any money laundering activities.
- Sudden disengagement from a long-standing relationship when enhanced due diligence is applied.

6.2. Transaction Behaviour

Unusual or Complex Payment Arrangements

- Involving unusual or complex payment arrangements without an apparent legitimate business or economical purpose.
- Transaction structure appears unnecessarily layered and designed to obscure the true origin of funds.
- Transactions involving the use of stolen or fraudulent payment instruments, such as payment cards that appear stolen, altered, or not issued in the customer’s name.

Involvement of Third Parties

- Transactions involving third parties as payers or recipients of payment or PMS, without legitimate business purpose. Examples include:
  - Payments received from a third party, who is not the owner of the funds, without legitimate business purpose.
  - Payments received from multiple unrelated third parties for the same transaction.
  - Payments of proceeds made to third parties overseas, despite the transaction being between a domestic buyer and seller, with no legitimate business purpose.

    - PMS delivered to a third party, who is not the owner or payer of funds, without legitimate business purpose.
    - Refunds paid to a third party, who is not the owner or payer of funds, without legitimate business purpose.
- Use of third-party cheques, third-party credit cards, precious metals (e.g., gold bars), precious stones (e.g., diamonds), or digital payment tokens.
- Introduction of third parties late in the transaction lifecycle without documented commercial rationale.
- Change in payer or recipient immediately following source of funds or ownership inquiries.

Suspicious Transaction Profiles or Amounts

- Transactions that are inconsistent with the usual profile of a customer, such as:
    - Transactions that appear to be beyond the customer's means based on their stated or known occupation or income, experience in the industry, or known share capital or period of incorporation.
    - Transactions that appear to be more than the usual amount or quantity for a typical customer.
    - Transaction purposes that are not aligned with the known or expected operations of the business.
- Series of transactions in different names.
- Transactions that do not consider the value, size, and/or colour of the precious stone, precious metal, or precious product.

Overpayment and Refund Requests

- Overpayment and requests for refunds of excess amounts to a third party or in cash.
- Large transactions that are cancelled shortly after deposits or full payment are made, resulting in refunds. For example, a customer may pay in cash and request a refund via cheque or make a credit card payment and request the refund in cash or another form.
- Payment made via virtual assets and refund is requested by other means to the customer or to a third party.

Unusual Transaction Volume or Frequency

- Numerous transactions by a customer, especially over a short period, where each transaction is not substantial, but the cumulative total is significant.
- Transactions involving virtual assets, especially where ownership cannot be easily traced to the customer.

Suspicious Online Transactions

- Indicators of suspicious online payment card-not-present transactions, such as:
    - Multiple online orders with the same shipping address but different payment cards, potentially indicating the use of stolen or fraudulent cards.
    - Same payment account but different shipping addresses, which could suggest the use of stolen payment card information shared among accomplices.
    - Same Internet Protocol (IP) address for online orders made around the same time with different payment cards, which may signify criminal activity using fraudulent payment cards.
    - Reattempting transactions with smaller amounts after an initial decline, which may indicate card testing to assess limits and available balances.

6.3. Supplier Behaviour

Lack of Transparency or Documentation and Forgery

- Inability to provide information for due diligence and record-keeping purposes.
- Provides forged, fraudulent, or false identity documents.
- Contracts, invoices, or other trade documents provided have vague or missing descriptions, appear counterfeit (including false or misleading information), include resubmission of previously rejected documents, or are frequently modified or amended.
- Supplier requests that normal business records not be kept.

Secrecy, Suspicious Origins and Products

- Supplier is unusually concerned with the business's Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), or Counter Proliferation Financing (CPF) policies.
- Supplier attempts to maintain a high degree of secrecy with respect to the transaction. Examples include:

    - Unwillingness to identify beneficial owners or controlling interests, where this would be commercially expected.
    - Requests for payments to be made through money services businesses or other non-bank financial institutions without apparent legitimate business purposes.
    - Vague or refusal to provide information on the reason for selling or buying PMS or about the origin of the items.
- Supplier's origins or the material's declared country of origin appears to be fictitious.
- Entity or any of its counterparties appear to import precious metals and stones that originate from a country with limited production or no mines at all.
- Precious metals (especially gold) originating directly or indirectly from conflict-affected or high-risk areas (CAHRA), including routing through neighbouring or intermediary countries to disguise true origin.
- Repeated changes in the declared country of origin across invoices, certificates, or shipping documents.
- Reliance on unverifiable or weak origin documentation, including unsupported "mine-of-origin" claims.
- Use of private refinery letters or unverifiable assurances instead of internationally recognized responsible sourcing documentation.
- Gold sourced or transited through jurisdictions known for weak supply-chain controls, illicit gold production, or conflict financing.
- Frequent re-routing of shipments, including unnecessary transshipment hubs without economic rationale.
- Shipment of recycled or secondary gold presented as newly mined without supporting evidence.
- Rough diamonds are not accompanied by a valid Kimberley Process certificate, for example:
    - No Kimberley Process certificate attached to the shipment of rough diamonds.
    - The Kimberley Process certificate is forged or appears to be forged.
    - The Kimberley Process certificate has an unusually long validity period.

Adverse Media or High-Risk Association

- Supplier is traced to a credible or verifiable negative news or criminal activities.
- Entity's owners, shareholders, authorized signatories, or any of its counterparties have been the subject of adverse news from a trusted media source.
- Supplier appears to be related to a high-risk country or territory, or entity associated with risks for money laundering or terrorism activities, or a person designated as a terrorist.
- Supplier transports PMS through a country or territory designated as "high risk for money laundering or terrorism activities" without apparent economic reason.

Other Behavioural Red Flags

- Supplier appears to be in a hurry to complete the transaction or is willing to sell PMS at a rate significantly lower than their typical sale value.
- Supplier does not appear to understand the DPMS sector or lacks the appropriate equipment or finances to engage in regulated activity in the DPMS sector.
- Supplier appears uninterested in or uninformed about the structure or transactions of their PMS business.
- Supplier lacks operational infrastructure, staffing, or financial capacity commensurate with declared high trade volumes.

6.4. Supplier Transaction Behaviour

Inconsistent Transaction Profiles

- Transactions that are not consistent with the usual profile of a supplier, including:
    - Over or under-invoicing, structured or complex transactions, multiple invoice requests, or high-dollar shipments that are over or underinsured.
    - Transactions that are excessive given the amount or quality of the goods or the potential profit from the sale of PMS.
    - Consignment size or type of PMS shipped that appears inconsistent with the capacity of the exporter or importer (e.g., shipments or transshipments that do not make economic sense).
    - Misclassification of gold purity, weight, origin, and value on customs declaration forms.
    - The transaction involves the use of front or shell companies, which have no real operating activity. For example, the entity's ownership structure appears to be doubtful or obscure, or the entity refuses to provide additional information when requested.

Third-Party Involvement

- Transactions in which third parties are involved, either as payers or recipients of payment or PMS, without an apparent legitimate business or economical purpose. Examples include:
  - Funds paid to a third party who is not related to the supplier, without a legitimate business purpose.
  - PMS delivered from a third party who is not related to the supplier, without a legitimate business purpose.
- Circular movement of goods or funds between related suppliers, intermediaries, or counterparties without clear economic rationale.

Virtual Assets Transactions

- Transactions involving virtual assets, especially when the ownership of the virtual assets cannot be easily traced to the regulated dealer and supplier.
- Supplier unable to provide a clear and verifiable documents supporting the source and the origin of the virtual assets.

6.5. Proliferation Financing Related Red Flags

Inconsistent or Evasive Behaviour

- Vague and resistant when additional information is sought.
- Hiding relationships between legal persons using nominees and shareholders with complex structures.
- PMS trade structures with unclear end-use, end-user, or ultimate destination of value.

Mismatched Activity

- Activity mismatches the entity line of business or end-user information mismatch with the business profile.
- Mismatch in the transaction value and the customer’s financial profile.

High-Risk Geographies & Unusual Routes

- Transactions involving higher-risk countries or jurisdictions.
- Shipment takes a circuitous route, or transaction takes a circuitous route.

Inconsistencies in Information

- Inconsistencies in trade documents, financial flows, destinations, ports, addresses, etc.
- Declared value of goods not matching with the shipping documents.

7. Case Studies

Case Study 1: <u>Precious Metals & Stones as Substitute Currency and Store of Value</u>

Synopsis

Domestic analysis of reported cases in Country A reflected the use of gold and diamonds as substitutes for cash by criminal networks involved in drug trafficking. The review noted that a member of the criminal network purchased gold and diamond jewelleries and gold bars using mixed payment methods, including cash, over several days. The individual requested for separate invoices for each item, ensuring that each individual purchase that involved cash payment fell below the reporting threshold. However, the cumulative total value made during the period of purchase was significantly high. Furthermore, when asked to provide information related to the purpose of purchase and source of funds, the individual failed to provide clear explanations and was evasive. The analysis also noted that the individual had visited multiple other DPMS where request for additional information regarding the purchases resulted in cancelation of transactions by the individual to avoid any scrutiny. Subsequent to purchases made, some of the gold and diamond jewelleries as well as the gold bars were sold back to the secondary market through wholesalers and scrap dealers at discounted prices, while others were retained. Some of the proceeds of the resale were then introduced into the financial system through third-party accounts and the remaining were used for further purchases. When analysed, the overall pattern indicated that the metals and jewelleries were being utilized to convert illicit funds into portable assets that were later liquidated in a manner intended to obscure the origin of criminally obtained funds.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Frequent purchases of PMS in quantities that does not align with the customer's profile or declared purpose*
- *Structuring transactions through various invoices or payment options to avoid scrutiny*
- *Hesitation or unwillingness to offer adequate details regarding the source of funds or purpose of purchase / transaction*
- *Abrupt cancellation of purchase / transaction once checks are initiated by the DPMS*
- *Rapid resale of newly purchased PMS via secondary or wholesale channels*
- *Use of third parties to process payments or collect proceeds of resale without clear rationale*

Supervisory Expectations

- *Evaluate whether the customer's behaviour and transaction patterns align with valid PMS trading or retail activity*
- *Apply enhanced scrutiny in instances where PMS appear to function as a substitute for cash or serve as means on storing value*
- *Re-evaluate the customer's risk profile when transaction patterns change or differ from anticipated behaviour*
- *Where reasonable grounds for suspicion arise, escalate internally for assessment to file a suspicious transaction / activity report*
- *Maintain sufficient documentation to ensure PMS traceability and demonstrate the application of a risk-based approach*

Case Study 2: <u>Gold Smuggling & Trade-Based Money Laundering (TBML)</u>

Synopsis

A recently established trading company ABC General Trading LLC, with a licence to engage in the trade of non-specialized goods, started conducting regular transactions related to gold bullion and scrap gold, shortly after its establishment. The activities listed on the company's trade license did not specify precious metals trading. For several weeks ABC General Trading LLC kept acquiring and selling gold from/to various DPMS, such as wholesalers and refiners, predominantly using cash for payment. Every cash transaction was well below the reporting threshold, despite the considerable volume in aggregate. When counterparties began to inquire about the source of funds and requested for documentation, the company offered invoices and certificates that seemed authentic initially but had discrepancies in dates, weights and stated purity. In cases where ABC General Trading LLC was selling gold to refiners, transportation-related documents evidenced routes through an additional third country without any clear commercial rationale, prior to arriving for refining. When asked for justification, the company cited 'logistical convenience' and 'shipment consolidation'. Post refinement, the gold was found to be sold to other trading companies overseas at prices that significantly varied from market rates. Proceeds from these sales were then transferred to bank accounts in the jurisdiction where ABC General Trading LLC was domiciled, however funds were credited to affiliated companies instead of its own account. Overtime, several DPMS counterparties started to notice unusual activities whereby the company did not show any interest in margins, rather it was more focused on speed of execution. Also, the company reportedly collected gold on behalf of different companies on numerous occasions. Analysis of suspicious transaction and activity reports noted that the company amended documentation frequently post completion of transactions. It was found that the cash used for the purchase of gold was the proceeds of crime committed abroad and the gold trading activity was used to convert illicit funds into portable, low-volume, high value goods which were transferred for resale abroad. Proceeds of resale were then introduced into the financial system by way of wire transfer from various counterparties domiciled in various jurisdictions.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *The nature, scale and frequency of transactions are inconsistent with the customer's declared profile (as can be evidenced through licenses, at times) and stated purpose of business*
- *Ambiguous justifications for trade activity with no documentations to substantiate the same*
- *Persistent reliance on cash as form of payment with unverifiable claims to rationalize dependency*
- *Lack of commercial rationale for transaction values*
- *Inconsistencies in documentation that suggest that the trade isn't genuine*
- *Complex trade routes which add costs and delay without reasonable justification*
- *Disproportionate transaction scale when compared with operational footprint*

Supervisory Expectations

- *Evaluate the customer's business profile and stated transaction purpose along with its operational footprint to ensure consistency with the nature, scale and frequency of purchases*
- *Undertake enhanced due diligence on the customer where inconsistencies arise*
- *Take reasonable steps to identify the source of funds and origin of gold*
- *Seek clarification on documentation discrepancies and ensure it substantiates the transactions' commercial rationale*
- *Where there is third-party involvement, the role of the third-party, the relationship with the customer and associated risk should be identified and evaluated. Unjustified third-party involvement should not be treated as routine*
- *Monitoring of the customer's activity over time is mandated whereby anomalies should prompt for risk assessment and potential escalation*
- *Where reasonable grounds for suspicion arise, escalate internally for assessment to file a suspicious transaction / activity report*
- *Maintain sufficient documentation to ensure PMS traceability and demonstrate the application of a risk-based approach*

Case Study 3: <u>Retail-Level Misuse of Diamonds & Jewellery for Drug Trafficking</u>

Synopsis

An organized criminal group, engaged in drug trafficking, was found accepting diamonds, gemstones and jewellery as payment (in place of cash). These assets were then transferred up the network to serve as settlement for drug supplies and outstanding debts. Those part of the criminal network who received the diamonds and gemstones as form of payment periodically converted the assets into cash through retail jewellery outlets and this is done in small, incremental amounts to avoid triggering threshold-based reporting. At the time of sale, the jewellery is presented as personal belongings with no consistent justification provided for continual transactions.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *The customer continually engages in resale of diamonds and jewellery over a period without any apparent personal justification (e.g. no association with a specific life event or liquidation)*
- *Gradual transaction scaling whereby jewellery is sold in small amounts that appear to be deliberate, particularly where aggregate volume is significant*
- *Resale consists of diamonds and jewelleries that always appear to be newly acquired or lightly worn and is sold immediately suggesting circulation rather than personal utilization*
- *Indications of viewing jewelleries as purely fungible asset with minimal interest shown for design or replacement value*
- *Customer avoids payment methods that involves regulated financial institutions*
- *Customer becomes evasive when asked basic questions about ownership or origin*

Supervisory Expectations

- *Identify anomalies that may appear beyond individual transaction size and assess frequency, pattern and cumulative behaviour*
- *Evaluate repeated resale activity to identify inconsistencies with the customer's profile and declared circumstances*
- *Instances where jewellery appears to function as a substitute for cash should warrant additional scrutiny*
- *Internal escalation should take place where resale activity appears structured or lacks economic rationale*
- *Where reasonable grounds for suspicion arise, escalate internally for assessment to file a suspicious transaction / activity report*
- *Maintain sufficient documentation to demonstrate how patterns were identified and assessed, inclusive of the application of a risk-based approach.*

Case Study 4: <u>Gold as a Substitute for Cash and a Laundering Vehicle</u>

Synopsis

A criminal syndicate involved in large-scale drug production uses gold as both payment within the organisation and a vehicle to launder illicit proceeds. By purchasing gold from prospectors and small traders using drug-derived cash, often at discounted rates, the group converts illicit funds into a portable, high-value commodity. The gold is accumulated as nuggets and bullion, portioned out to members as remuneration, and resold to unrelated dealers, where proceeds appear as legitimate commercial income. Because gold can be refined, melted, or commingled, its illicit origins become difficult to trace, enabling the syndicate to store, transport, and monetise value across jurisdictions while appearing to conduct legitimate DPMS-sector transactions.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Repeated cash-based purchases of gold in amounts that appear inconsistent with the customer's profile, particularly where the customer shows no sensitivity to market price fluctuations.*
- *Acquisition of gold from informal or undocumented sources, including prospectors, small-scale miners or unregistered traders, where origin information and supporting documentation cannot be substantiated.*
- *Rapid resale of gold to unrelated DPMS or trading entities shortly after purchase, with minimal or no commercial rationale, holding period, or value addition.*
- *Statements or behaviours indicating the use of gold as a method of remuneration or settlement, rather than for conventional commercial purposes—suggesting gold functions as a fungible, currency like asset.*
- *Accumulation or movement of substantial quantities of physical gold without the presence of legitimate business infrastructure (e.g., trading premises, storage facilities, refining arrangements or operational staff).*
- *Mismatch between the scale of gold trading activity and the declared business profile, financial capacity or economic circumstances of the customer.*
- *Vague, evasive or incomplete explanations regarding source of funds or source of gold, including reluctance or inability to provide documentation relating to cash origin or gold acquisition.*

Supervisory Expectations

- *Determine whether the customer's buying and selling patterns reflect genuine trading activity or appear structured primarily to convert cash into gold as a value-transfer mechanism.*
- *Apply proportionate enhanced due diligence where gold is purchased using cash, sourced from informal suppliers, or accompanied by weak or unverifiable origin documentation.*
- *Identify short holding periods, rapid resale, or commercially irrational profit margins that may indicate attempts to legitimise illicit funds.*
- *Ensure the scale, frequency, and nature of gold transactions align with the customer's declared business model, financial capacity, and operational footprint.*
- *Where multiple indicators suggest gold is being used as a substitute for currency or to launder proceeds, escalate internally and consider filing a suspicious transaction report.*
- *Retain clear records evidencing customer risk assessments, review of transaction purpose and justification, and the reasoning behind decisions to proceed, escalate, or report.*

Case Study 5: <u>Illicit Gold Trade through Wholesale Trading</u>

Synopsis

A precious metals wholesaler in a major trading hub conducts high-volume gold transactions through multiple bank accounts but consistently relies on large cash withdrawals to purchase gold from various suppliers. Although the business appears to operate legitimately, most purchases are settled in cash, suppliers are recorded generically as "private individuals," and little identification or origin verification is collected. Claimed sources such as scrap jewellery are inconsistent with the volumes supplied, and intelligence later indicates links to stolen jewellery, black-market gold and criminal networks. The wholesaler also structures transactions into sub-threshold tranches and uses intermediary entities, including a front company with minimal infrastructure, to fragment documentation and obscure counterparties. While individual transactions seem normal, the overall pattern shows a system designed to introduce illicit gold into the formal supply chain and convert criminal proceeds into seemingly legitimate revenue.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Repeated or unusually high-value cash withdrawals that are rapidly used to purchase gold, particularly where the scale of cash activity is inconsistent with the profile of a wholesale dealer.*
- *Suppliers routinely documented as private persons despite supplying commercial-scale quantities of gold, coupled with limited or no identification information.*
- *Gold transactions intentionally broken into smaller tranches to fall below reporting or due-diligence thresholds, especially where the pattern reflects deliberate avoidance of AML/CFT controls.*
- *Failure to obtain, verify, or assess the source of gold, particularly when suppliers claim to provide "scrap" volumes that exceed what would reasonably be expected from retail or personal sources.*
- *Individuals or small-scale collectors presenting quantities of gold that materially exceed their stated operational capacity, financial profile, or known business activity.*
- *Introduction of loosely connected or affiliated trading companies, often with minimal infrastructure, to fragment the transaction chain and distance the wholesaler from the original supplier.*
- *A wholesale trader relying primarily—or exclusively—on physical cash for gold purchases despite having established banking relationships or access to standard payment channels.*
- *Minimal or no CDD procedures, lack of beneficial ownership verification, or absence of a risk-based approach proportionate to the scale of gold trading activity.*

Supervisory Expectations

- *Wholesale DPMS must identify and verify all suppliers and counterparties, including establishing beneficial ownership where applicable.*
- *Declared sources of gold particularly claims involving "scrap" or personal holdings must be evaluated for plausibility relative to the quantity supplied. Where volumes indicate organised or commercial supply chains, enhanced scrutiny and documented justification are expected.*
- *Repeated transactions intentionally calibrated below reporting or due-diligence thresholds should be recognised as an indicator of elevated ML/TF/PF risk.*
- *Given that cash-intensive wholesale procurement presents heightened risk, DPMS must apply enhanced measures—such as additional verification, origin-of-funds enquiries, and more frequent monitoring—commensurate with transaction size and frequency.*
- *DPMS should understand the purpose, ownership, and economic rationale of intermediaries involved in transactions. Structures that introduce unnecessary layers or obscure the true supplier or payer must be treated as high-risk and subject to additional scrutiny.*
- *Wholesale DPMS must retain records demonstrating risk assessments undertaken, enquiries made regarding the source and ownership of gold, justification for proceeding with higher risk transactions, escalation and decision-making processes applied. Documentation should allow supervisors to trace gold flows and verify that a risk-based approach was followed.*
- *Where pattern of activity suggests the laundering of illicit gold, conversion of criminal proceeds, or the use of wholesale trading to facilitate anonymity, DPMS must escalate internally and consider filing a suspicious transaction/activity report even when individual transactions appear commercially rational or threshold-compliant.*

Case Study 6: <u>Use of Jewellery Merchant to Launder Narcotics Proceeds</u>

Synopsis

A diamond merchant in a major trading centre becomes a conduit for an organised criminal group involved in narcotics trafficking, receiving large payments in cash, money orders and cashier's cheques, often structured across multiple instruments, to purchase high-value diamonds and jewellery. The jeweller maintains incomplete or inaccurate records, fails to capture the true source of funds or the actual purchaser, and disregards reporting obligations, enabling illicit cash to be converted into portable, easily transferable assets. These diamonds and jewellery are subsequently moved or resold by the criminal network, distancing them from their criminal origin and facilitating the integration of drug proceeds into the legitimate economy.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Repeated high-value purchases of diamonds or jewellery funded through large cash payments, money orders or cashier's cheques, including payments made using multiple instruments in a structured manner.*
- *Customer demonstrates reluctance to provide information on the source of funds or identity of the actual purchaser, or attempts to use third parties without clear commercial rationale.*
- *Customer shows unusual urgency to complete transactions or avoids routine questioning about purpose, ownership, or intended use of the items purchased.*
- *Customer displays minimal interest in the design, quality or characteristics of jewellery, suggesting that the purchase is value-driven rather than personal or commercial.*
- *Failure to properly identify or verify customers, or recording transactions under incorrect or incomplete names.*
- *Transaction documentation that does not reflect the true nature, amount or source of funds.*
- *Customer attempts to alter documentation or requests that normal business records not be maintained.*
- *Evidence of structuring transactions to avoid triggering CDD, reporting or record-keeping obligations.*
- *Customer, associates or payment sources are linked to adverse media, criminal activity, or known involvement in narcotics trafficking.*

Supervisory Expectations

- *DPMS must identify and verify the true purchaser and payer, including assessing beneficial ownership where third parties are involved. Structuring payments through multiple instruments or intermediaries should trigger enhanced scrutiny.*
- *High-value purchases involving cash, money orders or cashier's cheques require DPMS to make reasonable enquiries regarding the legitimacy and origin of funds, with documentation retained to evidence such assessments.*
- *Repeated high-value purchases broken into smaller tranches or paid through multiple instruments should be treated as potential structuring and reassessed as part of the customer's ML/TF risk profile.*
- *DPMS are expected to maintain complete, accurate and contemporaneous records capturing purchaser identity, payment method, source-of-funds information and the rationale for the transaction, in line with regulatory obligations.*
- *Rapid resale, inconsistent explanations, third-party involvement, or implausible customer profiles must be escalated internally for review. DPMS should reassess risk ratings and determine whether escalation to SAR/STR filing is appropriate.*
- *Where a pattern of activity indicates the use of jewellery purchases to convert narcotics proceeds into portable assets or launder illicit cash, DPMS must file a suspicious transaction/activity report—even where individual transactions appear technically compliant.*

Case Study 7: <u>Use of Trade Documentation to Facilitate Cross Border Laundering</u>

Synopsis

A criminal syndicate in South Asia uses a network of shell companies across multiple jurisdictions inclusive of a UAE free-zone entity licensed as a general trading company to launder proceeds from fraud and cyber-enabled crime. The general trading company in the UAE engages in substantial gold trading activity without clear authorisation, operational substance or demonstrated expertise in PMS. The company issues invoices for gold bullion purchases and resales to related companies overseas, supported by banking transfers and trade documentation that give the appearance of legitimate cross-border commodity activity. However, no physical gold ever moves, and there is no evidence of shipments corresponding to the invoiced quantities.

Illicit funds are transferred into the UAE entity's bank account under the pretext of paying for gold, after which further transfers are made to another group company as supposed settlement for "refined bullion supply." In parallel, DPMS counterparties notice that the general trading company frequently requests pro forma invoices and trade confirmations but rarely completes actual collection of gold. The overall pattern reveals a classic trade-based layering scheme in which falsified gold trading documentation is used to disguise and circulate criminal proceeds through the international financial system.

Key Red Flags

Particular indicators (as listed below, but not limited to), especially when occurring in combination, should serve as alerts:

- *Misalignment between licensed activity and actual trading activity which may indicate the use of a front or shell entity to facilitate illicit financial flows.*
- *Frequent requests for pro forma invoices, trade confirmations or export-related papers with no consistent intention to take physical delivery of gold or complete settlement.*
- *Repeated revisions of documents in relation to weights, purity, values, or counterparties indicating potential fabrication, concealment or back-dating of trade activity.*

Supervisory Expectations

- *As part of due diligence measures, assess whether the licensed activity of the customer, operational footprint and commercial capability reasonably permits the scale and nature of PMS trading observed.*
- *Ensure escalation where material discrepancies exist between licensed activities and actual trade behaviour.*
- *Invoice-only trade should be escalated and reported where appropriate.*
- *Repeated requests for pro forma invoices, trade confirmations or purchase documentation in absence of corresponding settlement or collection of goods should warrant a reassessment of customer risk, scrutiny of business relationship and trigger internal escalation.*
- *Instances where payments flow through multiple intermediaries / affiliates across jurisdictions should trigger further scrutiny to identify rationale, ownership and legitimacy of each intermediary.*
- *Where trade pattern indicates use of invoiced-only gold trading to layer illicit proceeds, DPMS must escalate internally and consider submitting a suspicious transaction / activity report.*

7.1. Additional Case Studies on Money Laundering Involving Gold or Gold Sector[12]

Case Study 8: <u>Smuggling/Undervaluation Scheme Using Scrap Gold</u>

The United States Homeland Security Investigations (HIS) uncovered a smuggling / undervaluation scheme with scrap gold upon entry to the United States (US). From January 2012 to November 2013, a US importer (ultimate consignee) was smuggling scrap gold into the US from countries in Central America at undervalued prices and subsequently providing payments to the exporters at overvalued amounts. During this time frame two Central American companies sent scrap gold with a total declared value of approximately USD 6.4 million to the US importer yet during that same period wire transfers valued at approximately USD 24 million where sent back to the Central American companies for those imports. The owners of the US business were arrested and charged with conspiracy to commit money laundering using customs violations as a predicate offence.

Case Study 9: <u>Proceeds of Alleged Fraud Involved in the Gold Market</u>

A financial intermediary operating in refining and trading of precious metals sent a suspicious transaction report (STR) to the Money Laundering Reporting Office Switzerland (MROS), the Swiss FIU, in April 2014. The reporting financial intermediary is one of the world's largest processors of precious metals and is considered among the top three in Switzerland. Behind the decision of the financial intermediary to send an STR, was the publication of 'open source' information indicating that a customer had been arrested following an investigation relating to fraud, forgery of documents, drug trafficking and money laundering. After undertaking due diligence, the financial intermediary could not exclude the possibility that the assets (i.e. the gold that was to be refined) were the proceeds of crime. The STR related to the CEO and representative of a Spanish company specialising in buying retail gold with a turnover of more than EUR 1100 million in 2013. The company described itself as a very professional trading company for gold investments.

A US private equity firm specialising in buying and building companies controlled at 51% of the company. The remaining 49% belonged to a European fund, of which the CEO and the representative of the Spanish company held 49%. The company was active in the sale of gold bullion and, more recently, in acquiring jewellery and other gold pieces in order to refine and transform them in gold bullion. In 2009, its turnover was less than EUR 150 million while the following year, in 2010, it was more than EUR 500 million. In 2012, the turnover doubled from that of 2010 and was approximately 1000 million. The Swiss financial intermediary and the company were bound by a contract, which provided for both the refining of gold and the marketing and sales on behalf of the company. Based on the information provided by the financial intermediary and information held by the Swiss FIU, there was a question as to whether there were reasonable grounds to suspect that the concerned assets (i.e. the gold) were the proceeds of crime. In order to receive more information MROS sent two information requests to foreign FIUs. Unfortunately, only one foreign FIU answered the information request. The other FIU, the most important from the point of view of the relevance of the information, did not respond. Finally, the STR was forwarded by MROS to the competent law enforcement authority (LEA) in Switzerland. Before starting a preliminary investigation, the LEA waited on the results of the information request and, in particular, on more information about the investigation conducted on-site and about the reliability of the information concerning the alleged crimes. Meanwhile, the aforementioned company went through bankruptcy proceedings.

[12] Source: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML-TF-risks-vulnerabilities-associated-with-gold.pdf

Case Study 10: <u>Proceeds of Alleged Fraud Involved in the Gold Market</u>

The United States Homeland Security uncovered a scheme where a jewellery businessman hired a burglary ring to rob customers of previously purchased jewellery. The jewellery businessman would sell jewellery to customers and then hire an organized burglary ring and provide them the details of the jewellery to be stolen. The information provided by the jewellery businessman contained detailed product descriptions including the residential address of the customers. The burglary ring would then target both the jewellery the customer recently purchased as well as other items of value. During an HSI undercover operation, the jewellery businessman purchased allegedly stolen jewellery from an undercover agent and indicated that the jewellery would need to be melted and sold as scrap. The jewellery businessmen was arrested and charged with money laundering and sale of receipt of stolen goods.

Case Study 11: <u>A Gold Smuggling Case of Bangladesh</u>

A smuggler used air route for this crime. He came from Riyadh in Saudi Arabia to Dhaka, Bangladesh by Saudi Airlines. The smuggler's luggage was scanned and found to contain items consistent with metal goods. After opening the luggage, two bottles of a well-known soft drink were found in a carton. Each bottle contains 6 gold bars of investment quality; each gold bar was wrapped with foil paper. The luggage also contained two 135 gr bars of luxury soap, each soap contained a gold bar weighing 100 gr. In the smuggler's trouser pocket, were 77 gold chains and 2 gold earrings with a total weight of 240 gr. The authorities did not receive intelligence on this event prior to the detection. The smuggler was passing the 'green' channel. The duty officer scanned his luggage as a routine check and found the presence of the gold. Bangladesh has a unique operating environment when it comes to the gold market. In recent times no gold has been legally imported into Bangladesh but still the gold market is operating.

The smuggling of gold, either for domestic consumption or as a transit point for other countries, has replaced the lack of legal importation. This is despite the possibility of the death sentence for smuggling gold. Hundi or hawala13 are the most practiced method of moving value in the country in relation to the movement of gold. Analysis by Bangladesh Law enforcement concerning the movement of gold has established that Dubai, Mascot and Riyadh are the primary wholesale markets of gold. The gold is purchased from those markets and smuggled to Bangladesh, or via Bangladesh to other parts of the world. It has been established that, on occasion, such gold is used in the barter for arms or drugs. The money used to purchase the gold is sent either by currency smuggling or Hundi however little is known about the people responsible for this. On occasions it has been established that gold is smuggled to Bangladesh as a final payment to legal businesses where the partial payment owing has been undertaken legally. On other occasions people would smuggle gold to Bangladesh for purely economic reasons, in order to profit from the different market prices of gold globally.

Case Study 12: <u>Smuggling of Gold and Jewellery from Special Economic Zones</u>

Special Economic Zones (SEZ) are designated areas that have been created to enhance trade and in particular increase exports for the purpose of earning foreign exchange. Imports into a Special Economic Zones are allowed duty free. However due to the relaxed rules governing SEZ, these zones are also vulnerable to money laundering and tax evasion activity. Background: Directors of the companies identified in this case study were operating in the SEZ and had extensive contacts in the gold trade in India for more than 25 years. They had previously been investigated for gold smuggling and were also known to have committed customs/foreign exchange and income tax violations. One of the directors was also the owner of a gold manufacturing and trading company operating in Dubai. Modus Operandi: Companies A and B located inside a SEZ were authorised to manufacture and to trade in gold jewellery. This involved importing gold in either bullion form or as semi-finished jewellery from foreign jurisdictions. Generally, due to the special nature of SEZ there is no examination made by the authorities when the goods are imported or exported. These companies had opted for self-certification of the export goods as long as the activity met certain conditions. Representatives of companies X and Y (mostly run by families) would travel abroad and select jewellery in demand in the Indian market. This jewellery would be paid for at the time of purchase in the foreign jurisdiction in which it was bought. It would then be imported into the SEZ by the companies operating there recorded as jewellery for either scrapping or further finishing.

After customs clearance the goods would be moved from the airport to SEZ (a distance of 20 km). On the way, either the employees of the relevant company or one of the directors replaced the sealed imported packets with certain other sealed packets containing brass, scrap metal or other imitation jewellery. The jewellery that had been imported was then taken and sold to customers in legitimate gold markets. The sealed packets containing the brass, scrap metal or other imitation jewellery was self-certified as gold and studded jewellery and subsequently exported. These exports were to their own related companies with remittances being received as required by law. This scheme was made possible due to the absence of even random checks on exports of jewellery from SEZ. The Directors would charge their customers in INR 25 (Indian rupees) per gram of gold as a delivery charge and also offered commission of INR 5 per gram to the people coordinating the buyers in India. Magnitude: During the investigation DRI (Directorate General of Revenue Intelligence, India) seized 79 kg of gold jewellery valued at approximately USD 3 million. Examination of intercepted export consignments declared to contain 190 kg gold jewellery with a value of USD 7 million were found to contain scrap metal. DRI seized cash close to USD 100 000. Further 30 kg gold jewellery belonging to a related company was seized valued at USD 1.2 million. A total volume of doubtful imports covered were USD 100-120 million. The total quantum of customs duty evasion amounted to USD 10 million in addition to evasion of other taxes.

Case Study 13: <u>A Gold Smuggling and Money Laundering Case - Zimbabwe</u>

The Tunisian FIU received a Suspect Transaction Report (STR) related to a person X whose bank account registered a large amount of funds by means of cash remittances in short period of time and sought to withdraw the money in form of US dollar cash. Information gathered by the FIU as part of its analysis revealed that person X was linked to a network of gold smuggling. In country A, gold is a regulated sector overseen by the Central Bank. Enquiries established that person X procured gold by different illicit ways, particularly gold smuggled through land frontiers and robbery. Person X refined the gold into ingots and gave it to air hostess A. Air hostess A had access to all the airport zones and was able to avoid the customs and police controls. Air hostess A left the ingots supplied to her in a toilet near the gates and made a telephone call to smuggler/gold courier Y and told him where she had placed the ingots. Smuggler/gold courier Y retrieved the ingots and flew to country T. Once there, smuggler/gold courier Y delivered the ingots to person Z in return he received payment and returned to country A where he shared the profits derived from gold smuggling with person X. A month later the Tunisian FIU received additional information on person X. On this occasion person X had used the account of a company which he owned to try and disguise his identity. This was a more sophisticated scheme to conceal the nature of the transaction however the bank was able to detect the transaction because they had already flagged his name after the first STR. Person X had deposited an amount of ZAR 2.39million (approximately USD 239 000) into his company's account where, soon thereafter a converted US dollar amount was transferred to a third party telecommunications company.

Investigations by the FIU revealed that, after depositing the South African rand into his company's account instead of seeking to withdraw the amount in the form of US dollar cash, as he had wanted to do in his earlier activity; he instead transferred the amount, in batches, over a few days, to the telecommunications company to purchase mobile air-time in bulk quantities. Investigations revealed that person X was purchasing bulk airtime on behalf of airtime vendors in and around Kwekwe (Zimbabwe) and that person X made the purchases using the funds that he deposited as South African rand into his company's account, and which could now be transferred as US dollar. Person X would deliver the airtime to the airtime vendors in Kwekwe, who gave him instant cash, in US dollar. Through this method, person X had achieved his objective, to convert a large amount of South African rand cash into US dollar. Person X would then use the USD cash to make gold purchases, which he smuggled and sold outside the country.

Case Study 14: <u>Facilitation of Gold Smuggling and Money Laundering via Third-Party</u>

A Suspect Transaction Report (STR) was received by the FIU relating to person Z from bank B. Bank B had become suspicious after person Z had made several large cash deposits, in South African rand, into the bank account of a company that he owned and controlled. The deposits were followed by withdrawals of the amount in US dollars. The total amount involved was USD 6.6 million.

Investigations by the Zimbabwe FIU revealed that person Z had been conducting the transactions on behalf of a well-known gold dealer, in return for a commission. Person Z's friend person Y, was known to be involved in illegally buying gold from illicit suppliers and then smuggling the gold for re-sale out of the country. Estimates based on the amount of USD 6.6 million involved in this case, suggests that over one tonne of gold was illegally acquired, and smuggled out of the country.

<u>Case Study 15: Gold used as Justification for Cross-Border Funds Movement – Costa Rica</u>

A company operating in country A frequently sent representatives to country B offering services to buy gold, jewellery and precious stones / metals above local market prices. As a consequence of this activity, high quantities of funds were transferred from country A to country B with the reason given that the funds will be used to buy gold. The funds were then withdrawn from financial institutions in country B as either cash or cheques very soon after the funds transfer were made. Little was known about the movement of the merchandise purchased. The same organisation organised a significant event held at a luxurious hotel in country B, advertising an intention to buy gold. However, few customers were present at the event. Monies (of unknown source) said to be surplus to the cost of holding the event were then sent back to country A or sent to other countries where the company did not operate, with the argument that they would be used for similar events.

8. Glossary of Terms

Term	Definition
Bearer Negotiable Instruments / Cash Equivalents	Monetary instruments that function like cash and allow value transfer without normal banking traceability including cashier's cheques, money orders, postal orders, treasury bills, bearer bonds, bearer negotiable instruments, promissory notes, or similar instruments that can be transferred without identifying the underlying owner. Cash equivalents count toward the AED 55,000 threshold for covered transactions.
Beneficial Owner	The natural person who owns or exercises ultimate effective control over the customer, or the natural person on whose behalf the transactions are conducted; including any person who exercises ultimate effective control over a legal person or legal arrangement, whether directly or through a chain of ownership, control, or other indirect means, and who is identified, whether one or more, in accordance with the Executive Regulations of AML/CFT/CPF Law.
Business Relationship	Any ongoing commercial or financial relationship established between Financial Institutions, Designated Non-Financial Businesses and Professions, and their customers in relation to activities or services provided by them.
Committee	National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations.
Concerned Authorities	The governmental entities concerned with the implementation of any provision of this Decree by Law within the UAE.
Conflict-Affected and High-Risk Areas (CAHRA)	Countries or regions affected by conflict, weak governance, corruption, sanctions exposure, or widespread illegal mining activities that heighten ML/TF/PF risks in the PMS supply chain. Gold or gemstones originating from, routed through, or associated with CAHRA require enhanced scrutiny.
Covered Transactions	A transaction (single or multiple related payments) whose value is AED 55,000 or above, or which involves cash equivalents or structuring designed to avoid the threshold, thereby triggering the mandatory application of full AML/CFY/CPF measures under the UAE's AML/CFT/CPF law.
Crime	The crime of Money Laundering and the predicate offences related thereto, or the financing of terrorism, or the proliferation financing.
Customer Due Diligence (CDD)	The process of identifying and verifying the information of a Customer or Beneficial Owner, whether a natural or legal person or a legal arrangement, as well as identifying the nature of their business, the purpose of the business relationship, and the ownership structure and control thereover, including ongoing monitoring procedures.
Customer	Any natural or legal person, or legal arrangement, who establishes or seeks to establish a business relationship with Financial Institutions, any of the Designated Non-Financial Businesses and Professions, or Virtual Asset Service Providers.
Designated Non-Financial Businesses and Professions (DNFBPs)	Any person engaged in one or more of the commercial or professional activities or businesses, as specified in the Executive Regulations of AML/CFT/CPF Law.
Egmont Group	The Egmont Group is an intergovernmental body of 159 Financial Intelligence Units (FIUs), which provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism (ML/TF).

Term	Definition
Executive Office	The Executive Office for Control and Non-Proliferation, concerned with the implementation of targeted financial sanctions within the UAE.
Executive Regulations or AML/CFT/CPF Resolutions	Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing
FATF	The Financial Action Task Force is an inter-governmental body that 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.
Freezing	The taking of an action without prior notice or involvement of the owner, Customer, or the affected Party.
FSRBs	FATF-Style Regional Bodies are regional intergovernmental organisations which promote and assess the implementation of internationally accepted AML/CFT policies and regulations.
Financial Group	A group of financial institutions that consists of holding companies or other legal persons exercising the control over the rest of the group and coordinating functions for the application of supervision on the group, branch, and subsidiary level, in accordance with the international core principles for financial supervision, and AML/CFT policies and procedures.
Financial Institution	Any person engaged in one or more financial activities or operations determined by the Executive Regulations of the AML/CFT/CPF Law, on behalf of or for the benefit of a customer.
Financing of Terrorism	Any of the acts defined in Clause (1) of Article (3) of the AML/CFT/CPF Law.
FIU	Financial Intelligence Unit
Funds	Assets or properties, however acquired, of any type or form, tangible or intangible, movable or immovable, electronic, digital, or cryptographic, including national and foreign currencies, legal documents, and instruments of whatever form, including electronic or digital forms, evidencing the ownership of such assets or properties, or shares or rights therein; as well as economic resources deemed as assets of any kind, including oil and other natural resources and all rights pertaining thereto, whatever their value or means of acquisition; together with bank credits, cheques, payment orders, shares, securities, bonds, bills of exchange, letters of credit, and any proceeds, profits, or other income derived or resulting therefrom, which may be used to obtain any financing, goods, or services.
High Risk Customer	A customer who represents a risk either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by Financial Institutions, or Designated Non-Financial Businesses and Professions, or the Supervisory Authority.
Illegal Organisations	Organisations whose establishment is criminalised or which exercise a criminalised activity.

Term	Definition
Intermediary Account	Corresponding account used directly by a third party to conduct a transaction on its own behalf.
Intermediary / Third-Party Payer or Recipient	A person or entity (other than the customer or supplier) used to make or receive payments, collect goods, or execute parts of a transaction. Use of intermediaries without clear commercial rationale is a red-flag indicator of ML/TF/PF risk.
Kimberley Process Certification Scheme (KPCS)	An international certification regime governing the trade in rough diamonds, requiring participating countries to ensure that shipments of rough diamonds are conflict-free and accompanies by a valid Kimberley Process Certificate. DPMS dealing in rough diamonds must verify KPCS documentation as part of their CDD and supply-chain controls.
Law (or "AML/CFT/CPF Law")	Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing
Law Enforcement Authorities	The federal and local authorities entrusted, pursuant to the provisions of AML/CFT/CPF Law and their applicable legislation, with combating, investigating, detecting, and gathering evidence in respect of the offenses, including Money Laundering, Predicate Offences, the Financing of Terrorism, and the Proliferation Financing.
Legal Arrangement	Trusts or other similar arrangements.
MENAFATF	MENAFATF is 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 international AML/CFT standards. The UAE is one of the founding members of MENAFATF.
Means	Any means used or intended to be used for the commitment of an offence or felony.
Money Laundering	Any of the acts defined in Clause (1) of Article (2) of the AML/CFT/CPF Law, including its commission through digital systems, Virtual Assets, or cryptographic technologies.
Non-Profit Organisations (NPOs)	Any organized group of a continuing nature for a definite or indefinite duration, consisting of natural or legal persons or a legal arrangement, not aimed at profit, which collects, receives, or disburses funds for charitable, religious, cultural, educational, social, solidarity, or other purposes that fall within the scope of benevolent acts.
Politically Exposed Persons (PEPs)	Natural persons who are or have been entrusted with prominent public functions in the UAE or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following: 1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which include: a- Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP. b- Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.

Term	Definition
Predicate Offense	Any act constituting a felony or misdemeanour, including the financing of terrorism, the proliferation financing, and evasion of direct and indirect taxes, in accordance with the applicable legislation of the UAE, whether committed within or outside the UAE, provided that such an act is punishable in both countries.
Proceeds	Funds derived, directly or indirectly, from the commission of any felony or misdemeanour, including profits, privileges, economic interests, and other benefits derived therefrom, and any equivalent Funds that have been converted, in whole or in part, into other Funds.
Proliferation	The illicit and unauthorized trade, as regulated under the applicable legislation in the UAE, in materials, systems, equipment, components, programs, or technology contributing to the production or development of Weapons of Mass Destruction, related technology, or their delivery means, including any act stipulated in Clause (3) of Article (3) of this Decree by Law.
RBA	A Risk-Based Approach is a method for allocating resources to the management and mitigation of ML/TF/PF risk in accordance with the nature and degree of the risk.
Registrar	The competent authority responsible for supervising the economic or trade register of the various types of establishments registered in the UAE, as regulated by the legislation in force in the UAE.
Sanctions Committee	The UN Security Council Committee established as per resolution numbers 1988 (2011), 1267 (1999), 1989 (2011), 2253 (2015), 1718 (2006) and all other related resolutions.
Sanctions List	A list wherein individuals and terrorist organisations, which are subject to the Sanctions imposed as per the Security Council Sanctions Committee are listed, along with their personal data and the reasons for Listing.
Settlor	A natural or legal person who transfers the management of their own Funds to a Trustee pursuant to a Trust Instrument.
Shell Bank	Bank that has no physical presence in the country in which it is incorporated and licensed and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
Supervisory Authority	The federal and local authorities entrusted under the legislation with the supervision of the financial institutions, designated non-financial businesses and professions, virtual asset service providers, and non-profit organizations (NPOs); or the competent authorities responsible for granting approval to engage in an activity or profession, where no specific supervisory authority is designated by the legislation.
Suspicious Transactions	Transactions involving funds for which there are reasonable grounds to suspect that they constitute Proceeds of any felony or misdemeanour, or are related to Money Laundering, Financing of Terrorism, or Proliferation Financing, whether such transactions were executed or merely attempted.

Term	Definition
Terrorist	Any natural person, whether within or outside the UAE, who intentionally commits any of the following acts: 1. Commits or attempts to commit a Terrorist Act by any means, whether directly or indirectly. 2. Participates as an accomplice in a Terrorist Act. 3. Organizes a Terrorist Act or incites others to commit it. 4. Participates with a group of persons acting with a common intent to commit a Terrorist Act for the purpose of expanding terrorist activity or to commit such act, knowing the group's intention.
Terrorist Organization	A group of two or more persons, whether within or outside the UAE, that has committed a terrorist act, directly or indirectly, or has threatened to commit it, aims, plans, or seeks to commit it, or promotes or participates in its commission, whether directly or indirectly, regardless of its name, form, place of establishment, location, activity, or the nationality or residence of its members; including any organization recognized as a Terrorist Organization under any other law.
Targeted Financial Sanctions (TFS)	The freezing of funds and the prohibition of making them available, directly or indirectly, for the benefit of any natural or legal person or organization designated by resolutions issued by the Cabinet regarding Terrorist Lists, or by the United Nations Security Council under Chapter VII of the Charter of the United Nations concerning the prevention and suppression of terrorism and its financing, as well as the prevention, suppression, and halting of proliferation and its financing.
Trade-Based Money Laundering (TBML)	The process of disguising the proceeds of crime and moving value through trade based transactions, including under/over invoicing, misrepresentation of quality, false documentation, layering through involvement of multiple intermediaries.
Transaction	Any disposal or utilization involving Funds or Proceeds, including, inter alia, deposit, withdrawal, transfer, sale, purchase, lending, exchange, mortgage, or donation.
Trust	A legal relationship whereby the Settlor places Funds under the control of a Trustee for the benefit of a Beneficiary or for a specific purpose, and such Funds are deemed separate from the Trustee's own property, while the title thereto remains in the name of the Settlor or another person on behalf of the Settlor.
Trustee	A natural or legal person vested with the rights and powers granted thereto by the Settlor or by the Trust, authorized thereby to manage, utilize, and dispose of the Settlor's Funds in accordance with the conditions imposed by either of them.
Virtual Assets	Digital representation of value that may be digitally traded or transferred and may be used for payment or investment purposes, excluding digital representations of fiat currencies, securities, or other Funds.
Weapons of Mass Destruction	Weapons capable of inflicting harm on a large number of persons and posing a threat to human life and the natural environment through their catastrophic effects, such as nuclear, biological, chemical, or radiological weapons.
Without Prior Notice	The taking of an action without prior notice or involvement of the owner, Customer, or the affected Party.

Term	Definition
Virtual Asset Service Providers (VASPs)	Any natural or legal person who, as a commercial activity, conducts one or more of the virtual asset activities specified in the Executive Regulations of this Decree by Law or conducts transactions related thereto, on behalf of or for the benefit of another natural or legal person.
Wire Transfer	Financial transaction conducted by a Financial Institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether or not the transferor and the beneficiary are the same person.