الإمارات العربية المتحدة
وزارة الإقتصـــــاد

Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations

Guidelines for Designated Non-Financial Businesses and Professions

Supplemental Guidance for Dealers in Precious Metals and Stones

May 23, 2019

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

11.4.1 Introduction

Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* (the "AML-CFT Decision") identifies dealers in precious metals and precious stones (DPMS)[1] as Designated Non-Financial Business and Professions (DNFBPs), when they engage in carrying out any single monetary transaction, or several transactions which appear to be interrelated, whose value is equal to or greater than AED 55,000,[2] and subjects them to specific AML/CFT obligations under the AML/CFT legislative and regulatory framework of the United Arab Emirates.

Recent studies[3] have concluded that the nature of precious metals and precious stones (PMS), and the characteristics of the markets in their trade, make them inherently highly vulnerable to misuse or exploitation by criminals for the purpose of money laundering and the financing of terrorism. DPMS are likewise vulnerable to ML/FT risks.

Among the reasons noted for this vulnerability are the facts that:

- 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/FT, 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

[1] 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 precious stones" and "dealers in precious metals and precious 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.
[2] For convenience, such transactions will be referred to throughout the text of this Supplemental Guidance as "covered transactions."
[3] See, for example, *Money Laundering and Terrorist Financing through Trade in Diamonds*, Financial Action Task Force/OECD/Egmont Group of Financial Intelligence Units, October 2013; *Implementing AML/CFT Measures in the Precious Minerals Sector: Preventing Crime While Increasing Revenue*, International Monetary Fund, August 2014; *Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold*, FATF/Asia Pacific Group on Money Laundering, July 2015; and *Professional Money Laundering*, FATF, July 2018.

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 the 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 in regard to the ML/FT risks, due-diligence requirements, and the red-flag indicators associated with their trade, increase the vulnerability of DPMS to exploitation by criminals and terrorists.

Further complicating the picture 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. The UAE's ML/FT National Risk Assessment (NRA) found that:

> "The overall large size and openness of the UAE Financial Sector, its geography, the large proportion of foreign residents, the use of cash in transactions, and *the highly active trade in gold and precious metals and stones*, were also inherently open to ML/TF abuse by criminals."[4]

Transactions involving PMS, and the exploitation of DPMS, have been identified as a ML/FT typology commonly used by professional money launderers and organised crime groups.[5] The NRA has also identified professional money laundering (PML) as being one of the highest crimes/threats in relation to ML in the State, and illicit trafficking in stolen and other goods, together with smuggling, among the medium-high threats. Accordingly, among the sectors the NRA has identified as having among the highest inherent ML/FT vulnerability in the UAE (onshore) is that of DPMS. This sector was also identified as having medium-high inherent ML/FT vulnerability in the Financial Free Zones.

Given all of the above, it is of critical importance that DPMS are well acquainted with their CDD obligations under the UAE's AML/CFT legislative and regulatory framework, as well as with the various risk factors and indicators that can help them to identify and report suspicious transactions. While the former have already been covered in depth in the *Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations*

[4] *Brief on the National Risk Assessment (NRA) in the United Arab Emirates*, Government of the UAE, May 2018 (italics added).
[5] See, for example, *Professional Money Laundering*, op. cit., pp. 15, 17.

Guidelines for Designated Non-Financial Businesses and Professions, it is the intent of this supplemental guidance to cover the latter in greater detail with respect to dealers in precious metals and precious stones.

11.4.2 Summary of AML/CFT Obligations for DPMS

All DPMS which qualify as DNFBPs are required by the AML-CFT Law and the AML-CFT Decision to fulfil certain obligations which constitute the basis of an effective risk-based AML/CFT programme, in respect of covered transactions. These obligations include:

- Identifying and assessing ML/FT risks (see Guidelines Section 4);
- Establishing, documenting, and updating policies and procedures to mitigate the identified ML/FT risks (see Guidelines Section 5);
- Maintaining adequate risk-based customer due-diligence (CDD) and ongoing monitoring procedures (see Guidelines Section 6);
- Identifying and reporting suspicious transactions (see Guidelines Section 7);
- Putting in place an adequate governance framework for AML/CFT, including appointing an AML/CFT Compliance Officer, and ensuring adequate staff screening and training (see Guidelines Section 8);
- Maintaining adequate records related to all of the above (see Guidelines Section 9); and
- Complying with the directives of the Competent Authorities of the State in relation to the United Nations Security Council resolutions under Chapter VII of the Charter of the United Nations, as well as in relation to *Cabinet Decision No. (20) of 2019 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* (see Guidelines Section10).

The ultimate purpose of these measures is to establish a reliable paper trail of business relationships and transactions, and to trace the true beneficial ownership and movement of assets, in order to prevent DPMS from being exploited for the purposes of money laundering and/or the financing of terrorism, and to aid the Competent Authorities of the State by reporting suspicious transactions.

The sections below provide additional guidance specific to DPMS, in regard to the identification of risk, customer due diligence, and the identification and reporting of suspicious transactions.

11.4.3 What are Precious Metals and Precious Stones (PMS)?

While the definitions of precious metals and precious stones may vary somewhat depending on region, the most generally accepted classifications internationally, based on factors such as quality, intrinsic value, and rarity, consider the precious metals to consist of gold, silver, and the so-called platinoid metals (principally platinum and palladium); and precious stones 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 reflected in the federal legislation of the UAE, 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.[6]

Taking into consideration the above, and without prejudice to any pre-existing or subsequent definitions included in any federal law or regulation of the UAE, the definitions of precious metals and precious stones for the purpose of this supplemental guidance include, but are not limited to, those materials falling under the following categories:[7]

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

- Diamonds (rough) of any weight in carats;
- Diamonds (polished), with a minimum weight of 0.3 carats per stone if loose, or a minimum weight of 0.5 carats per any single stone mounted in a setting (whether of one or more stones);

[6] 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.
[7] See *Decision of the Council of Ministers No. (45) of 2018 on the Executive Regulation of Federal Law No. (11) of 2015, on the Control and Stamping of the Trade in Precious Stones and Precious Metals*, Annexes 1 and 2.

- 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, with a minimum diameter of 3 millimeters per bead;
- Strung or mounted in a setting (whether of one or more beads), with a minimum diameter of 10 millimeters per any single bead.

Other

The above definitions notwithstanding, for the purpose of applying AML/CFT measures in respect of covered transactions, DPMS should also consider PMS to include any object concerning which at least 50 percent of its monetary value is comprised of PMS. Furthermore, it should also be recognised that DPMS 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 (although they may be of high value in some cases), may nevertheless be subject to risks of ML/FT or other predicate offences (e.g. fraud) similar to PMS. Such materials may include:

- A variety of high-value industrial metals, including so-called conflict minerals (for example, wolframite, cassiterite, and coltan), cobalt, and other platinoid metals (e.g. rhodium, etc.);
- A variety of semi-precious gemstones (e.g. amethysts, opals, jade, and others);
- Synthetic, treated, or artificial gemstones (diamonds, emeralds, rubies, sapphires, pearls).

While this supplemental guidance focusses on the ML/FT risks associated specifically with PMS, DPMS should also take a similar risk-based approach to the application of AML/CFT measures in respect of covered transactions involving these other types of metals and stones (since they can, in some situations, also be considered to pose ML/FT risks similar to those of PMS). In other words, the criterion for applying the required AML/CFT measures relates to the carrying out of monetary transactions which meet the threshold amount of AED 55,000.

11.4.4 Who is a Dealer in Precious Metals or Precious Stones (DPMS)?

A dealer in PMS may be considered to be any natural or legal person (or legal arrangement), or their employee or representative, who engages, as a regular component of their business activities, in the production and/or trade of precious metals or precious

stones, whether in raw, cut, polished, or elaborated (mounted or fashioned) form. Production and/or trade in this context includes any of the following acts involving raw/rough or processed/finished PMS:

- Extraction (whether by mining or other method), refining, cutting, polishing or fabrication;
- Import or export;
- Purchase, sale, re-purchase or re-sale (whether in primary, secondary, or scrap markets);
- Barter, exchange, or other form of transfer of ownership;
- Loan or lease arrangements (e.g. sale-leaseback, consignment, or memorandum sales);
- Possession (whether permanent or temporary, for example, as part of a fiduciary, warehousing, collateral, or other safekeeping arrangement; or under contract for a specific purpose such as cutting, polishing, refining, casting or fabrication services).

The above-referenced conditions are irrespective of whether the transaction is wholesale or retail; whether it is direct or indirect (such as through a broker or other intermediary); whether it is between natural or legal persons or legal arrangements, including any other DPMS; and whether the PMS are traded physically or virtually (for example, via certificates, on electronic exchanges, or via internet), irrespective of where or by whom the physical goods are warehoused, held in safekeeping, or delivered.

11.4.5 When Do the AML/CFT Obligations Apply to DPMS?

Under the AML-CFT Law and the AML-CFT Decision, DPMS are obliged to apply the required AML/CFT measures when they qualify as DNFBPs. This occurs whenever they carry 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. Some examples of when application of the AML/CFT measures is (or is not) required are provided below for illustration purposes.

- 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 installment, 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 considered to be 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 considered to be 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 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 meet the threshold.

- A diamond cutting and polishing firm wishes to buy a consignment of KP-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 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 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 <u>not</u> obliged to apply the AML/CFT 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 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.

As long as DPMS carry out covered transactions, they are obliged to fulfil all of the AML/CFT programme obligations specified in the AML-CFT Decision, including appointing an AML/CFT compliance officer, implementing adequate staff/employee AML/CFT training, establishing effective internal controls, maintaining adequate records related to those covered transactions, and reporting suspicious transactions, among others. Furthermore, it should be noted that certain of the AML/CFT obligations under the AML-CFT Law and AML-CFT Decision are independent of whether or not DPMS engage in covered transactions. For example, DPMS are obliged to comply with the instructions issued by the Competent Authorities in the State concerning the implementation of the decisions issued by the UN Security Council under Chapter VII of the UN Charter (see Guidelines, Section 10, International Financial Sanctions), at all times. DPMS should ensure they allocate adequate resources and have adequate procedures in place to apply the measures, as required.

11.4.6 Risk Factors of Specific Concern to Dealers in Precious Metals/Stones

The AML-CFT Decision specifies certain risk factors that should be taken into consideration by DNFBPs when identifying and assessing ML/FT risk at both the enterprise and the customer levels. General guidance on these risk factors is provided in Section 4.4 of the Guidelines.

In addition to these generalised risk factors, there are a number of additional risk factors which DPMS should be aware of and should take into consideration in identifying and assessing the ML/FT 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. Other risk factors relate to the nature and type of the customer or transaction involved.

Stage 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. DPMS may perform a wide variety of roles or functions relating to the trade in PMS, and in order to understand these roles and the potential ML/FT risks they entail, it is necessary to have a basic understanding of the stages of the supply chain. It should be understood that the supply chains for different PMS may have certain characteristics which are unique to that particular PMS or category of PMS. Furthermore, the supply chain is not necessarily a strictly vertical one, in that different participants may trade with each other in multiple directions at different stages of the chain, and certain stages may run concurrently or be skipped altogether. However, for the sake of convenience, these stages, and some of the major ML/FT risks to which each stage is vulnerable, may be 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 methods (as in alluvial manual collection). This stage may also include the sorting and grading of raw minerals, and their preparation for sale. Key ML/FT 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-, or false-invoicing and accounting fraud.[8] This stage is also vulnerable to numerous predicate offences, such as theft, embezzlement, smuggling, and bribery/corruption. Thus the

[8] References to this type of fraud throughout this section include but are not limited to misrepresentations of quantity, quality/purity, origin, or price, and the substitution of PMS with other (fake) materials, for the purpose of ML/FT..

extraction/production process may be used as a vehicle for both the creation of and the laundering of illicit proceeds.

- **Trading in raw minerals**. In this stage, raw ores or rough gemstones are obtained from the extraction source and traded by dealers. This stage of the supply chain may also involve the export and import of raw ores 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)[9], 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/FT risks, in that the number and variety of participants (including street vendors 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/FT 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);
  - Infiltration of criminal or terrorist organisations among raw mineral traders;
  - Prevalence of cash (or cash equivalent) transactions;
  - Vulnerability to smuggling.

- **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 ores, and cutting and polishing with respect to precious stones. This stage can also include the recycling of

[9] The Kimberley Process Certification Scheme (KPCS) is a United Nations sponsored international trade regime, aimed at preventing the entry into and circulation of so-called conflict diamonds in the international diamond market, through a certification system. The United Arab Emirates has been a participant in the KPCS since 2013.

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/FT risks at this stage include but are not limited to: the obscuring of traceability of PMS through the beneficiation process; trade-based ML; the prevalence of cash/cash-equivalent transactions; and vulnerability to commingling.

- **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/FT 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.

- **Retail trade**. In this stage, beneficiated PMS or finished goods (in particular 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/FT risks connected with commingling, as well as to the classic ML/FT risks associated with placement, layering and integration, and to predicate offences such as fraud, theft and robbery or embezzlement, among others.

Stages of the Supply Chain and Roles of DPMS[10]

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

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 measures, DPMS acting in any of the roles mentioned above should carefully consider factors such as customer risk, geographic risk, channel risk, and product, service and transaction risk (see Guidelines Sections 4.4.1, 4.4.2, 4.4.3 and 4.4.4). In particular, consideration should be given to such factors as:

- Counterparty/customer 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, has a poor transparency or corruption index, or is a known location for the operation of criminal or terrorist organisations);
- 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—see Guidelines Section 6.4.3)—particularly in relation to the locations where the transaction is conducted and the goods are delivered;
- 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 (see Guidelines Section 4.4.3, among others), 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 (see Guidelines Sections 4.4.5 and 4.5.4).

Geographic risk[11]

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

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

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. The types of risk profiles identified and assessed, and the resultant risk ratings applied to the customers (see Guidelines Section 4.5.1), should be used in determining the efficient allocation of AML/CFT resources, as well as the appropriate application of reasonable and proportionate risk-mitigation measures, including customer due-diligence measures (discussed below).

In assessing ML/FT risk 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/FT risk profiles based on their business models, standard market practices, and target customer segments, against which customers may be filtered and risk-rated. Whatever methods they choose, DPMS should clearly document them (including the rationale for their use), and apply them consistently across their business activities.

11.4.7 Customer Due Diligence (CDD) Guidance for Dealers in Precious Metals and Precious Stones

Together with the accurate identification and assessment of ML/FT 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 programme. The *Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations 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 study the related sections of the Guidelines

carefully. Nevertheless, there are some additional points that are of particular relevance to DPMS.

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 (see Guidelines Section 10, International Financial Sanctions), and for performing background checks on them to identify any potentially adverse information (including associations with PEPs, or financial or other crimes) about them. 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.

Second, a characteristic technique used in a variety of ML/FT 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). 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 speaking, 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. 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.

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.

11.4.8 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 example of ways in which they may do so include, but are not limited to:

- In cases of covered transactions (see Sections 11.4.4 and 11.4.5 above): 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.

11.4.9 ML/FT Typologies

As mentioned in the Guidelines (see Section 4.3 ML/FT Typologies), 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/FT 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/FT involving DPMS. These methods broadly align with the classical stages of the ML/FT process (i.e. placement, layering, and integration; see Guidelines Section 4.2, The Standard ML Model and Generic ML/FT Risks); 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/FT trends and typologies into their employment screening and compliance training programmes (see Guidelines Section 8.2, Staff Screening and Training), 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/FT, according to the Financial Action Task Force (FATF):[12]

- 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

[12] 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.

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.[13]

- 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.

- Laundering illegal PMS and/or the use of PMS to launder the proceeds of crime. As noted earlier (see Section 11.4.6), the PMS supply chain is complex and can involve multiple participants in each stage, with varying levels of control and numerous vulnerabilities to ML/FT 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 ML. 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.[14]

- 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

[13] 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.
[14] 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.

fairly easily. This is often done in conjunction with the other ML/FT 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.

11.4.10 Examples of ML/FT Cases

Example 1: **Financing drug trafficking with diamonds and ML through retail level**[15]

This case involved an organised criminal group that distributed drugs and controlled several low level (street-level) drug dealers in Canada. The higher placed distributor would distribute drugs to the street-level dealer and receive diamonds, gemstones and jewellery as payment, as well as cash. Likewise, the street-level drug dealer traded drugs for diamond jewellery and then traded up to the higher-placed drug dealer for more drugs and debt payments. The higher-placed drug distributor would then sell the diamonds and jewellery at small incremental amounts (CAD 3,000-CAD 8,000) to the jewellery market (retail jewellers) and in return would receive payment by way of cheque. The drug distributor also received high-end jewellery (watches) instead of payment for the illicit jewellery.

Example 2: ML involving jewellery as payment for drugs and as a means to store value[16]

This case involved a drug dealer/producer who sold drugs and traded drugs for collectively over USD1 million in stolen and purchased jewellery. The drug dealer who had strong industry, commodity, and market knowledge sold the least valuable jewellery as scrap to jewellers and bullion dealers. Jewellery that had some aesthetic or residual market value above the component parts was sold as estate jewellery to jewellers. In return, the drug dealer received cash, gold and silver bars and coins, and diamond jewellery. The drug dealer used some of the proceeds of crime from the sale of drugs and sale of jewellery obtained in trade for drugs to purchase specific diamond jewellery and gemstones items as a mean to store wealth. The drug dealer used appraisals to value the jewellery that was stored as wealth and to help negotiate fair prices for the resale of the jewellery in the market.

Example 3: Trading in gold to legitimise the proceeds of drug trafficking[17]

[15] *Money Laundering and Terrorist Financing through Trade in Diamonds,* op. cit., p. 87.
[16] Ibid., p. 90.
[17] *Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold,* op. cit., p. 8.

The United States Homeland Security Investigations (HSI) uncovered a scheme where illicit proceeds from a drug trafficking organisation were being used to purchase gold. A criminal organisation in the US was buying gold from various precious metals retailers using illicit proceeds from narcotics sales. The gold was then sold to a precious metals broker who then sold it to other businesses. The proceeds of the sale were then wired to a third party out of the US with links to the drug trafficking organization, thus completing the money laundering cycle.

Example 4: Use of gold as an alternative currency to pay drug syndicate members and to launder the proceeds of crime[18]

An investigation into a well-organised and resourced drug syndicate in Australia identified a former bank manager as the head of the operation. Allegedly, the suspect was involved in financing and facilitating the multi-million dollar cannabis and amphetamines production operation and was linked with several well-known criminals.

The head of the operation was suspected of laundering the proceeds from the drug syndicates through the purchase and sale of gold, the purchase of cattle and through gambling. Authorities believe the suspect used cash to purchase gold from prospectors at a reduced price and then sold the gold to unrelated businesses and declared it as legitimate revenue. Police located a large quantity of gold nuggets and AUD 161,000 cash hidden by the syndicate.

Those involved in the operation were paid well, and some received bonus payments in drugs and gold. One worker was paid a total of AUD 250,000 in cash, drugs and gold in the four seasons he was involved in the operation. Syndicate chiefs were paid more than AUD 300,000 each harvest, as well as being paid in gold bullion.

Commonwealth proceeds of crime action was taken against the offenders and resulted in the restraint of over AUD 4 million worth of assets, including rural properties, cattle, machinery, AUD 220,000 cash and a large quantity of gold. The law enforcement operation led to the arrest of number of syndicate members, who were subsequently charged and jailed for lengthy periods of time.

Example 5: Use of diamonds/precious stones by criminals as an alternate currency[19]

[18] Ibid., p. 10.
[19] *Money Laundering and Terrorist Financing through Trade in Diamonds,* op. cit., p. 87.

A drug courier/trafficker was found carrying CAD 40,000 worth of drug money. The courier's cash bag also contained a quantity of diamond jewellery and loose sapphire gemstones that collectively were valued at CAD 60,000. The jewellery had been appraised by a third party. The appraisal value listed the jewellery for its cash value, if sold at just below the wholesale price, demonstrating that the diamonds and gemstones were being used between criminals as an alternate currency.

Example 6: Wholesale gold trade used as cover for ML operation[20]

A wholesaler in precious metals (Wholesaler A) was known to the police to engage in money laundering. Wholesaler A held various bank accounts in Belgium, analysis of which showed that he mostly paid suppliers of precious metals in cash. Over the period of one year, a total amount in excess of EUR 800 million was withdrawn in cash. The account mainly received payments from a Belgian bank for purchases of bullion gold.

Wholesaler A's customers were mainly shops selling gold in Antwerp, private individuals, and intermediaries that were all recorded as "private individuals" in the company's accounts. Wholesaler A did not ask its customers for any identification, nor did he inquire into the origin of the gold. Enquiries established that much of this gold was said to have come from the black market (jewellery theft), as well as from criminal organisations linked to prostitution and drugs.

Wholesaler A paid for the gold in cash, and larger quantities of gold were split up so the price would never be more than the EUR 15,000 AML/CFT reporting threshold. One of Wholesaler A's suppliers, Company/Trader B also paid its gold suppliers in cash. In its financial records, Company/Trader B recorded the supplying companies as private individuals, without any form of identification. Company/Trader B was suspected to be a cover for the owners' illegal activities, i.e. laundering proceeds of crime by exchanging money. Other suppliers of Wholesaler A were also known to the police, leading to the suspicion that Wholesaler A was acting as a platform to launder criminal proceeds by providing anonymity and cash payments.

Example 7: ML through the gold trade by a narcotics cartel[21]

Thirty-one defendants face federal money laundering charges for their roles in a conspiracy that allegedly laundered more than USD 100 million in drug proceeds for the Mexico-based Sinaloa Cartel by purchasing gold, reselling it to companies in Florida and California, then

[20] Ibid., p.9 (as adapted).
[21] Adapted from *Strengthening the Security and Integrity of the Precious Metals Supply Chain*, op. cit., pp. 44-45.

transmitting the money from the United States to Mexico. Members of the organisation were routinely directed to the United States to collect narcotics proceeds, to use the money to purchase scrap and fine gold from local businesses, and to ship that gold to refineries based in Florida and California. The refineries in turn transmitted the cash value of the gold to co-conspirators in Mexico.

Example 8: Laundering the proceeds of narcotics trafficking through a jeweller[22]

A New York diamond merchant, Mr A, was arrested in 2006 and accused of being part of a conspiracy to launder about USD 270 million in drug profits. He was among 40 people indicted in the scheme orchestrated by an organised crime group, which ran drugs out of Detroit beginning in the 1990s. Mr A facilitated the purchase of jewellery utilising the drug proceeds of the other defendants in order to conceal the true nature, source and ownership of the funds involved in these transactions. After receiving payments in cash, money orders and cashier's cheques, amounting to hundreds of thousands of dollars for each payment, Mr A would fail to report these cash payments to the IRS or would falsify the records. Officials dropped the money-laundering charges against the jeweller as part of his plea agreement, but he was sentenced in 2008 to two-and-a-half years in federal prison for lying to investigators about his part in the multistate drug ring, and was also fined USD 50,000 and ordered to forfeit USD 2 million to the US government.

Example 9: Drug proceeds laundered through PMS smuggling operation[23]

A New York law enforcement operation targeted a ML method commonly used by Colombian drug traffickers. Using this method, drug traffickers and the money brokers who provided them with laundering services employed couriers to pick up cash and deliver it to gold jewellers and suppliers. The jewellers or suppliers exchanged the cash for gold, diamonds or other precious commodities, which were then smuggled to Colombia, either via couriers or hidden in cargo. Once the diamonds and gold arrived in Colombia, they would be sold for Colombian pesos, which were then delivered to the narcotics traffickers.

Roman Nektalov, owner of Roman Jewellers, operated a scheme to launder what he believed to be narcotics proceeds. Cooperating witnesses (CW) and under-cover law enforcement agents (UC) indicated that they and their associates had narcotics proceeds in the New York City metropolitan area, which they wanted to exchange for gold and diamonds for onward smuggling to Colombia. At trial, the Government presented testimony and audiotape recordings of meetings in which the CW, the UC and Nektalov discussed

[22] *Money Laundering and Terrorist Financing through Trade in Diamonds,* op. cit., p. 98 (as adapted).
[23] Ibid., p. 99.

Nektalov's sale of diamonds to the UC in exchange for cash believed by Nektalov to be drug money. The evidence showed that Nektalov met with the CW and the UC at Roman Jewelers to exchange a large number of diamonds for USD 500,000 in cash. After the diamonds were placed on a table in a back room where the transaction was to take place, federal agents entered Roman Jewelers, arrested Nektalov, and seized the diamonds. Nektalov was sentenced to 10 months imprisonment for ML.

Example 10: Perpetration of tax fraud and laundering of the proceeds through the diamond trade[24]

Over a three-month period, law enforcement officers observed Suspect A travel from an Australian-based airport to the offices of two diamond dealers. On each occasion, Suspect A left the diamond dealers' offices in possession of a plastic shopping bag which he had not taken into the dealers' offices. The following day, Suspect A deposited a large amount of cash into the account he had opened in the name of a fake charity, and transferred the funds to Israel.

Authorities alleged that most of the money laundered by Suspect A came from the cash sale of diamonds which had been imported illegally into Australia. Following the cash sale of the diamonds, the proceeds were collected by Suspect A and deposited into the account of the fake charity. The funds were then transferred back to the overseas-based diamond suppliers under the guise of charitable donations. This method facilitated the avoidance of sales tax on the sale of the diamonds and the payment of income tax on the profits from the sale.

Enquiries identified that three bank accounts in Israel and one in Sweden received funds sent by Suspect A and his family. A further two overseas-based accounts were identified. These accounts also received funds and both accounts were associated with diamond merchants in Israel and Belgium. These diamond merchants supplied wholesale diamonds to Australia.
Suspect A was convicted of conspiracy to defraud the Commonwealth and sentenced to five years imprisonment.

Example 11: Diamonds trader involved in corruption, drugs and arms trafficking[25]

In 2011, a bank submitted an STR to the Swiss FIU concerning his client X, who had made his fortune in the trade with diamonds and precious metals in Africa on behalf of counterparts in the Middle East and the European Union. After conducting research on an

[24] Ibid., p. 106.
[25] Ibid., pp. 113-114 (as adapted).

external database, the bank discovered that X and his company Y were subject to sanctions issued by the US authorities (OFAC Specially Designated Narcotics Trafficker Kingpin) for trafficking of weapons and drugs. X was also believed to be a member of a criminal organisation. A press article also suggested that X was involved in a case of arms trafficking, corruption of judges and ML in a country in South America, where he was known as a property developer.
Analysis by the FIU confirmed the bank's suspicion.

Example 12: Gold reshaped into common objects to avoid detection by customs (1)[26]

The United States Homeland Security Investigations (HSI) and Internal Revenue Service-Criminal Investigation (IRS-CI) uncovered a scheme related to gold being reshaped and exported as common objects like cones. From December 2001 through May 2003, Jaime Ross, owner of Ross Refiners, a gold refining business in Manhattan's Diamond District in New York, was selling bulk quantities of gold to an undercover agent posing in an undercover operation as a narcotics money launderer.

Ross would sell the gold, knowing that the currency used allegedly came from narcotics sales. Ross would recast the gold into cones and alter the colour of the gold to avoid detection while being smuggled to Colombia. Ross was arrested on 4 June 2003 and charged with money laundering and failing to declare the cash transaction relating to the sale of gold.

Example 13: Gold reshaped into common objects to avoid detection by customs (2)[27]

Under 'Operation Meltdown', United States Homeland Security Investigations (HSI) uncovered a carousel scheme in which jewellers were converting the proceeds from drug sales into the equivalent value in gold.

The scheme involved a criminal organisation with links to gold suppliers in the New York area that were laundering millions of dollars in drug proceeds. The HSI investigation disclosed that the exported gold from Colombia was described as 'gold pigments', and upon importation into the United States the same merchandise was then described as 'gold bullion'. The gold bullion was transported to New York, where jewellers cooperating with drug trafficking organisations disguised the gold as a wide range of common objects like wrenches, nuts, bolts, belt buckles and trailer hitches. These items were exported back to Colombia at a declared value far below the worth of their weight in gold. Upon arrival in

[26] *Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold,* op. cit., p. 12.
[27] Ibid., pp. 12-13.

Colombia, the same gold was recast into bullion and exported again to the US as 'gold pigment'.

The investigation of this case resulted in the arrest of 23 jewellers charged with money laundering and other arrests, along with the seizure of 140 kg of gold, more than 100 loose diamonds, USD 2.8 million, 118 kg of cocaine, 6 guns and two vehicles.

Example 14: Financing of Terrorism in Colombia involving the mining sector[28]

Columbian military and law enforcement officials carried out operations against terrorist organisations, including the Revolutionary Armed Forces of Colombia (FARC), which derived income from gold, tungsten and coltan mines. FARC collected funds by extorting different actors in the mining supply chain, including the imposition of entry and machinery use fees, and "work permit" charges to traditional miners and to gold mines. They also received income from allowing the transport and sale of precious metals. In another case, a narco-terrorist organisation took control of a territory where a gold mine was in production, extorting the owners by way of violence and forcing the community to transfer the ownership titles to them. They then used the mine illegally, selling gold to a legal business for cash, which was used to buy equipment, munitions, medicines, and other supplies to support their terrorist activities.

As a result of the law enforecement operations, involving more than 63 mines, terrorist organisations were prevented from siphoning off more than USD 8 million from the mining sector, and the organisations' networks of illegal finance and support were dismantled. The investigations resulted in numerous arrests (including 12 members of FARC) and the confiscation of illegal mining equipment, weapons, and tonnes of food supplies.

Example 15: Gold smuggling and laundering through cash and exchange houses[29]

The Zimbabwe FIU commenced an investigation based on a suspicious transaction report (STR) from a financial institution in Zimbabwe (Bank A). This STR reported that the subject, a holder of a personal bank account, attempted to make a cash deposit of ZAR 4.1 million (South African rand, equivalent to about USD 410,000) into his account and sought to immediately withdraw the money in US dollars. Prior to the attempted transaction, his account had been overdrawn, thereby raising suspicion regarding the source of the substantial cash deposit. The bank was not satisfied that the funds were from a legitimate source, and it declined to accept the deposit and immediately filed an STR with the FIU.

[28] Ibid., p. 16, and *Emerging Terrorist Financing Risks*, FATF/OECD, October 2015, p. 41 (as adapted).
[29] *Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold,* op. cit., pp. 15-16.

The FIU conducted an interview with the individual who explained that the money was proceeds from the sale of gold which he had purchased from small-scale miners and illegal dealers who operated in and around Kwekwe, one of Zimbabwe's gold producing regions. The Kwekwe region is dominated by small-scale licensed miners as well as illegal gold "panners," who prefer to make a quick sale and therefore sell to buyers such as the subject who pay cash on the spot. It was also asserted that gold buyers offer the small-scale and illegal miners not only cash on the spot, but also offer a more attractive price than the state licensed buyer, which withholds a percentage as a statutory levy.

The subject stated that he smuggled the gold to South Africa (with which Zimbabwe shares a border), where he would sell the gold to different buyers, including licensed gold millers, for cash. The subject indicated that his buyers, in turn, smuggled some of the gold from South Africa to Asia where they sold it to jewellers. The subject added that the attempted deposit was intended to enable him to exchange the South African rand (which he gets upon disposal of the gold in South Africa) for US dollars (the currency acceptable to the gold suppliers), which he would use to purchase more gold on the black market and continue the cycle.

On being asked how he disposed of his ZAR4.1million after his bank had declined to accept his deposit, the subject revealed that he exchanged the South African rand through black market currency exchangers in Harare. This case is one of many similar STRs which the Zimbabwean FIU has received and processed. While a few of the illegal gold dealers change their South African rand to US dollars through banks, many others prefer to change the South African rand on the foreign currency black market to avoid detection.

Example 16: Gold smuggling through physical "muling"[30]

Following a physical search of the bags of a suspected person (Person A) at Kabul airport, four packages of gold bars weighing 11.724 kilograms were found in his bags. Airport security cameras recorded that Person A had only one bag with him when he entered the airport terminal, and that the second bag was brought to the terminal by a second person (Person B). It was revealed that both persons entered the toilet of the terminal after one another, and after coming out of the toilet, one of them went to the airline's counter and handed over the bags. It was also noticed that after the bags were handed over at the airline counter, Person A went into the terminal hall, while Person B left the airport terminal.

Example 17: Laundering illegal diamonds through smuggling and financial hubs[31]

[30] Adapted from *APG Yearly Typologies Report 2018,* Asia/Pacific Group on Money Laundering, July 2018, p. 56.

Police in Antwerp investigated a massive diamond fraud in which a family smuggled diamonds worth an estimated EUR 1.3 billion over the course of several years. Most of the income from the scheme is thought to have been exported to Lebanon.

The investigation started with a warning from the state security service that the family had connections with known dealers in illegal diamonds. The diamonds were allegedly brought into Antwerp and the receipts then exported, both undocumented, to evade huge sums in tax. The illegal diamonds, including stones originating from conflict zones (possible conflict diamonds) were mixed with legal diamonds and the whole shipment KPC indicated that the origin of the diamonds was from multiple mining countries. The family managed to get around the Kimberley system by passing the stones through the United Arab Emirates and Switzerland before bringing them into Belgium. Meanwhile, the profits were laundered by means of false invoices and fake bookkeeping.

Example 18: Diamond smuggling via "mule" networks[32]

Mr. N, an Indian national who arrived on a flight from Dubai, was stopped for customs inspections by officials at a Moscow airport while attempting to pass through the Green Corridor for passengers who have nothing to declare. The ensuing luggage inspection and body search produced several pieces of jewellery (pendants and earrings) and a total of 30,401 natural diamonds valued at nearly RUB 4.7 million, all of which were confiscated.

—

South African police have arrested a man who they say swallowed 220 polished diamonds in an attempt to smuggle them out of the country. The man was arrested as he waited to board a plane at Johannesburg airport. Officials said a scan of his body revealed the diamonds he had ingested, worth USD 2.3 million. The man was travelling to Dubai. According to the information, authorities believe the man belongs to a smuggling ring. Another man was also arrested, attempting to smuggle diamonds in a similar way.

—

An investigation of a suspected tax evasion case of a woman who operated a small kindergarten led to the discovery of a diamond smuggling network. According to the tax authorities, the network operated in Israel, Belgium and Russia. Investigators found that the owner's husband had travelled abroad 245 times in the past eight years, on trips that usually lasted just two days. During the investigation, 15 men and women were arrested, all suspected of being involved in the smuggling ring. The suspects were relatives who allegedly carried out more than 500 such diamond operations with a value of hundreds of thousands of USD. They were allegedly paid USD 600 per trip plus travel expenses, and hid the diamonds inside private body parts.

[31] *Money Laundering and Terrorist Financing through Trade in Diamonds,* op. cit., p. 114.
[32] Ibid., pp. 118-120.

Example 19: Laundering drug proceeds through a wholesale jeweller located abroad[33]

US authorities indicted an offshore business engaged in the illicit black market peso exchange, an ML operation through which narcotics proceeds earned in the United States were exchanged for Colombian pesos and then used to purchase goods in the Colon Free Zone in Colon, Panama. During the course of the investigation, two natural persons were identified as major money launderers based in Panama. The two used a wholesale jewellery business and a related company, engaged in the sale of gold and silver jewellery and precious metals to many retail and wholesale customers throughout Central and South America, Europe, and the Middle East, to facilitate their illegal ML activities.

According to evidence presented in the case, drug proceeds from the United States were sent to Panama through cash pick-ups, wire transfers, cashier's checks and third party bank checks. Through the companies, which together did more than USD 100 million in business annually, the defendants knew that the primarily South American-based customers were laundering millions of dollars in drug money from the United States through bulk purchases of jewellery. According to court documents, the companies were heavily involved in the black market peso exchange. In signing the asset forfeiture order, a US District Court Judge found that "a primary modus was to sell jewellery to drug lords, knowing that it was being paid for with drug money, thus allowing them to convert dirty money into glistening clean jewellery." The assets seized from the wholesale jewellery company included approximately 468 boxes of gold and silver jewellery, as well as gemstones and watches, weighing ten tonnes.

Example 20: Third party gold smuggling syndicate used to launder proceeds of illegal drug sales[34]

In early 2014, the French police uncovered an international money-laundering network, used to launder the proceeds of the sale of cannabis in the Paris region of France. Moroccan dealers smuggled hashish to France and sold it at street level. An Indian national organised the collection of the cash proceeds from the street sales. This money collection (called ‘amana’ by the syndicate) was undertaken by so-called ‘salafs’ (mules), who were aware that they were dealing with the proceeds of the crime, but not of the crime itself. This was an intentional decision by the group to put some distance between the predicate criminal activity and the *salafs*. The *salafs* took their orders from the Moroccan drug dealers

[33] Ibid., p. 117.
[34] Adapted from *Money Laundering and Terrorist Financing Risks and Vulnerabilities Associated with Gold,* op. cit., pp. 6-8.

and supplied the money to the Indian national. The investigation estimated that in a six-month period the *salafs* collected well in excess of EUR 10 million. Whilst the Indian national kept a very low profile in France (he had no official income apart from his wife's social allowances, and lived in social housing in the suburbs of Paris), he held a number of valuable assets in India.

On receipt of the money, the Indian national arranged the transportation of the cash by car to Belgium where it was used to purchase gold and jewellery. The bulk of the cash was deposited in cash into the different accounts of companies associated with an identified gold trader and used to purchase gold from a wholesaler. False invoices generated by the Indian national (in the name of companies set up by him) were used to provide support for transactions involving the gold coins and ingots, as well as gold certificates, if authorities ever questioned the holder of the gold.

The investigation established two main routes used to move the gold to India. In the first instance the gold was transported to Dubai where it was sold to local people or Indian nationals (via a *hawaladar*). On the sale of the gold the Moroccan drug dealers were paid via controlled foreign exchange operations in Dubai. The physical gold was then smuggled into India with the assistance of an employee of a travel agency based in Dubai who recruited mules to undertake the work for a small fee amounting to approximately EUR 220. The investigations identified couples, elderly people, and on one occasion the use of a 'toddler' to undertake this activity. To make the gold easier to conceal, a jeweller transformed it by various methods, including mixing gold flakes with coffee, nickel electrolysis of jewels, and 100 g gold drops for internal concealment.

According to information, the gold was not smuggled to Dubai but officially exported and declared to customs, using the false invoices as a cover. Both the jewellery and the gold were sent to Dubai using false invoices and fake companies in the UAE. If the transactions were completed without intervention, the false invoices were destroyed; and if not, then they were used to support the activity. The investigation established that the gold trader kept official records for the sale of 190 kilograms of gold in 11 months, with a value of approximately EUR 6 million.

The Indian national used relatives to transport the gold to India and the UAE, with one of the relatives travelling more than 200 times to India and the UAE from 2008 to 2014 (two to three times a month). The head of the India syndicate controlled a travel agency in India, which provided flight tickets to the mules and sometimes fake invoices for the purchase of gold. An alternate route to transport the gold from Belgium to India was via the international airports of Bangkok and Singapore to a professional Burmese smuggler. The gold was then conveyed through Myanmar to India where it was sold.

Irrespective of the route used, from the moment the money was collected off the streets in France, it took five days for the money launderers to pay back their Moroccan silent

partners. The Indian syndicate's profit was based upon the conversion and resale of gold. By smuggling gold and avoiding taxes, the Indian syndicate was able to sell it competitively and still make a profit. The gold in question was purchased at EUR 31 per gram in Belgium and resold for EUR 36.32 per gram in Dubai or India. The Belgium gold trader received a fee of EUR 325 per kilogram, which equated to a profit of EUR 5,000 per kilogram for the syndicate.

This system used by the Indian syndicate was so profitable that the Indian gave up his normal commission on the money laundered. His only desire was to channel as much *amana* as possible in order to buy gold again and again. Thus he offered the unique opportunity for his Moroccan partner to launder his money at no cost.

11.4.11 Indicators of Suspicious Transactions for Dealers in Precious Metals and Precious Stones

From the examples provided above, it can be seen that criminals' methods are constantly evolving, and in many cases are specific to the particularities of a given market or a given type of trust and company services. The following list of red-flag indicators of potentially suspicious transactions is therefore by no means exhaustive.

DPMS are also reminded that the presence of one or more of the indicators below does not necessarily mean that a transaction involves ML/FT; however, it is an indication that enhanced due diligence or further investigation may be required, so that an appropriate determination can be made by the DNFBP's appointed compliance officer as to whether the transaction is suspicious or not.

The Business Relationship, Counterparty, or Customer:

- Suddenly cancels the transaction when asked for identification or information.
- Is reluctant or refuses to provide personal information, or the DPMS has reasonable doubt that the provided information is correct or sufficient.
- Is reluctant, unable, or refuses to explain:
  - their business activities and corporate history;
  - the identity of the beneficial owner;
  - their source of wealth/funds;
  - why they are conducting their activities in a certain manner;
  - who they are transacting with;
  - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).

- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.
- Is a designated person or organisation (i.e. is on a Sanctions List).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
- Actively avoids personal contact without sufficient justification.
- Is a politically exposed person, or has familial or professional associations with a person who is politically exposed.
- Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for doing business with the DPMS.
- Is located a significant geographic distance away from the DPMS, with no logical rationale.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction, or is unfamiliar with the details of the requested transaction.
- Makes unusual requests (including those related to secrecy) of the DPMS or its employees.
- Is prepared to pay substantially higher fees than usual, without legitimate reason.
- Appears very concerned about, or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Requests services (for example, smelting and reshaping of gold into ordinary-looking items, or re-cutting and polishing precious stones) that could improperly disguise the nature of the PMS or conceal beneficial ownership from competent authorities, without any clear legitimate purpose.

- Claims to be a legitimate DPMS but cannot demonstrate a history or provide evidence of real activity.
- Is a business that cannot be found on the internet or social business network platforms (such as LinkedIn or others).
- Is registered under a name that does not indicate that activity of the company is related to PMS, or that indicates activities different from those it claims to perform.
- Is a business that uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorised the transaction.
- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering, terrorism financing, or corruption risk.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense.
- Appears to be acting according to instructions of unknown or inappropriate person(s).
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for short-cuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Requests payment arrangements that appear to be unusually or unnecessarily complex or confusing (for example, unusual deposit or installment arrangements, or payment in several different forms), or which involve third parties.
- Provides identification, records or documentation which appear to be falsified or forged.
- Requires that transactions be effected exclusively or mainly through the use of cash, cash equivalents (such as cashier’s cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or other such payment methods), or through virtual

currencies, for the purpose of preserving their anonymity, without adequate and reasonable explanation.

The transaction:

- Involves the use of a large sum of cash, without an adequate explanation as to its source or purpose.
- Involves the frequent trading of PMS (especially diamonds and gold) or jewellery for cash in small incremental amounts.
- Involves the barter or exchange of PMS (especially diamonds and gold) or jewellery for other high-end jewellery.
- Appears structured so as to avoid the cash reporting threshold.
- Involves delivery instructions that appear to be unnecessarily complex or confusing, or which involve foreign jurisdictions with no apparent legitimate connection to the counterparty or customer.
- Includes contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Involves payments to/from third parties that do not appear to have a logical connection to the transaction.
- Involves merchandise purchased with cash, which the customer then requests the merchant to sell for him/her on consignment.
- Involves PMS with characteristics that are unusual or do not conform to market standards.
- Involves the unexplained use of powers-of-attorney or similar arrangements to transact business on behalf of a third party.
- Appears to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Involves a person acting in the capacity of a director, signatory, or other authorised representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries, when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.

- Involves several successive transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, especially when the nature of the merchandise or the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involves unexplained last-minute changes involving the identity of the parties (e.g. it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the goods, without a logical explanation.
- Involves circumstances in which the parties:
  - Do not show particular interest in the details of the transaction;
  - Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms;
  - Insist on an unusually quick completion, without a reasonable explanation.
- Takes place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.
- Involves unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involves indications that the counterparty does not have or does not wish to obtain necessary governmental approvals, filings, licences, or other official requirements.
- Involves any attempt by a physical person or the controlling persons of a legal entity or legal arrangement to engage in a fraudulent transaction (including but not limited to: over- or under-invoicing of goods or services, multiple invoicing of the same goods or services, fraudulent invoicing for non-existent goods or services; over- or under-shipments (e.g. false entries on bills of lading); or multiple trading of the same goods and services).

The Means of Payment:

- Involves cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or similar instruments), negotiable bearer instruments, or virtual currencies, which do not state the true payer, especially where the amount of such instruments is significant in relation to the total value of the transaction, or where the payment instrument is used in a non-standard manner.
- Involves unusual deposits (e.g. use of cash or negotiable instruments, such as traveller's cheques, cashier's cheques and money orders) in round denominations (to keep below the reporting threshold limit) to pay for PMS. The negotiable instruments may be sequentially numbered or purchased at multiple locations, and may frequently lack payee information.
- Is divided in to smaller parts or installments with a short interval between them.
- Involves doubts as to the validity of the documents submitted in connection with the transaction.
- Involves third-party payments with no apparent connection or legitimate explanation.
- Cannot be reasonably identified with a legitimate source of funds.