GUIDANCE NOTES ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

FOR

DEALERS IN PRECIOUS METALS AND STONES

MARCH 2020

1. INTRODUCTION

1.1 This Guidance is issued by the Financial Intelligence Authority (**FIA**) pursuant to s. 20(d) of the Anti-Money Laundering Act, 2013.

1.2 The Anti- Money Laundering Act, 2013 (the "**AMLA**") identifies dealers in precious metals and precious stones (**DPMS**)[1] as accountable persons and therefore imposes duties and responsibilities on them to prevent and detect money laundering and the financing of terrorism.

1.3 The purpose of this Guidance is to provide industry specific guidance for DPMS on their legal obligations for measures to deter and detect money laundering and the financing of terrorism activities. It provides clarity and an interpretation of the issues arising out of the AMLA and the AML regulations. This Guidance explains the most common situations under the specific laws and related regulations which impose Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) requirements. It is provided as general information only. It is not legal advice, and is not intended to replace the Acts and Regulations.

1.4 DPMS and other reporting entities should always refer directly to legislation when considering their statutory obligations. DPMS are responsible for continuously monitoring developments in the law and, where applicable, keeping their own internal procedures effective and up to date.

2. MONEY LAUNDERING/FINANCING TERRORISM (ML/TF) RISKS RELEVANT TO THE SECTOR

2.1 Recent studies have concluded that the nature of precious metals and precious stones (**PMS**), and the characteristics of the markets

[1] For the sake of convenience, the abbreviations PMS and DPMS will be used throughout the text of this Guidance to indicate the terms "precious metals and precious stones" and "dealers in precious metals and precious stones", respectively.

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 therefore equally 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/TF, 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, decentralized, and often cash-based markets for certain types of precious metals and stones (particularly for gold and diamonds, but for other PMS as well), often allowing them to be traded or exchanged with relative anonymity;
- The difficulty in tracing specific items, and the global nature of the markets for PMS, make it easier for criminals to exploit cross-border, multi-jurisdictional situations in order to obscure 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."*

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.

2.2 Uganda's ML/TF National Risk Assessment (**NRA**) found that a significant ML and TF risk exists in this sector as there has been a significant increase in illegal and informal gold mining activities in Uganda. These activities are conducted by both local and foreign nationals (from neighboring countries) which may result in the illicit dealing and smuggling of gold across borders with the proceeds likely to be laundered through the Ugandan financial system. The porous borders make it easy for cross border trading that goes on unlicensed and

unrecorded. Gold is highly valuable relative to its weight. This compactness makes it easy to smuggle and difficult to detect. Gold is virtually untraceable, odorless and can be held anonymously without need for records to be kept.

The NRA noted that the major risks of ML/TF and vulnerabilities stem from the following factors:

- Proximity to countries with illegal traffic of gold and other precious stones (e.g DRC), which are smuggled through Uganda;
- Publicly available information points to the illegal exploitation and smuggling of gold from DRC and the use of proceeds for laundering and funding other illicit activities, including the funding of terrorist organizations such as the ADF;
- Porous borders, non-effective controls at Entebbe airport and the risk of corruption is also a major risk factor;
- A process for the certification of origin of gold extracted from the region has been put in place by the countries of the region, but it is at its nascent stage and the regime is not yet complete;
- An estimated 90% of miners in Uganda are artisanal miners and they may tend not to officially declare the gold extracted, but to sell it in the "black market."
- Uganda is not a member of the Kimberley process certification scheme.

Given all of the above, it is of critical importance that DPMS are well acquainted with their obligations under the 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.

3. WHO IS A DEALER IN PRECIOUS METALS OR PRECIOUS STONES (DPMS)

3.1 For the purposes of this Guideline, a "dealer" in precious metals and stones means …. *"a wide range of persons engaged in these businesses, from those who produce precious metals or precious stones at mining operations, to intermediate buyers and brokers, to precious stone cutters and polishers and precious metal refiners, to jewellery manufacturers who use precious metals and precious stones, to retail sellers to the public, to buyers and sellers in the secondary and scrap markets."* This therefore also applies to Artisanal and small scale Miners (ASM).

Precious metals include, but are not limited to bullion, platinum, gold and silver coins, and jewellery made from same.

Precious stones include but are not limited to diamonds, rubies, precious and semi-precious stones and man-made gemstones.

Jewellery means objects made of precious metals and/or precious stones intended for personal adornment.

4. WHEN DO THE AML/CFT OBLIGATIONS APPLY TO DPMS

The AML/CFT law subjects its requirements to both mineral dealers and retailers when engaged in any cash transactions equivalent to or exceeding the amount of One Thousand Five Hundred currency points (equivalent to UGX. 30,000,000).

5. SUMMARY OF AML/CFT OBLIGATIONS FOR DPMS

All DPMS are required by the AMLA and the AML Regulations to fulfill certain obligations. These obligations include:

(1) Registration with the FIA
(2) Reporting suspicious transactions and certain cash transactions
(3) Undertake customer due diligence (CDD) measures
(4) Ascertain whether the customer is acting for a Third Party
(5) Record keeping
(6) Develop and implement internal control measures, policies and procedures to mitigate ML/TF risks
(7) Appoint a Money Laundering Control Officer
(8) No Tipping Off

5.1 Registration with FIA

In accordance with regulation 4 of the AML Regulations 2015, DPMS are required to register with the FIA for the purpose of identifying them as entities which are supervised by the FIA. They must also notify the FIA of a change of address of their registered office or principal place of business.

a) <u>How to Register</u>

The registration process is simple and free of charge. Registration forms are available on the FIA's website; www.fia.go.ug which, you may download, complete and have it delivered to FIA office, on Plot 6 Nakasero Road, 4th Floor Rwenzori Towers (Wing B).

5.2 Reporting suspicious transactions and certain cash transactions

By virtue of section 9 of the AMLA as amended, DPMS are required to report to the FIA if they suspect or have reasonable grounds to suspect that;

- A transaction or attempted transaction involves proceeds of crime or,
- A transaction or attempted transaction involves funds related or linked to or to be used for money laundering or
- A transaction or attempted transaction involves funds related or linked to or to be used for terrorism financing, regardless of the value of the transaction.

According to section 9(2) of the AMLA, the STR must be submitted within two (2) working days of the date the transaction was deemed to be suspicious.

According to Regulation 12(7) and (8) of the Anti-Terrorism Regulations 2016, you **must submit an STR to the FIA immediately** if a designated entity* attempts to enter into a transaction or continue a business relationship. **You must not enter into or continue a business transaction or business relationship with a designated entity.**

* A designated entity means any individual or entity and their associates designated as terrorist entities by the United Nations Security Council (UNSC). **You can access the Security Council of the United Nations List ("the UN list") on the UN website.**

a) Defining Knowledge and Suspicion

The first criterion provides that, before you become obliged to report, you must know or have reasonable grounds for suspecting, that some other person is engaged in money laundering or terrorism financing.

If you actually 'know' that your Customer is engaged in money laundering, then your situation is quite straightforward – the first

criterion is met. However, knowledge can be inferred from the surrounding circumstances, so, e.g., a failure to ask obvious questions may be relied upon to imply knowledge.

You are also required to report if you have *'reasonable grounds'* to suspect that the Customer or some other related person is engaged in money laundering or financing of terrorism. By virtue of this second, 'objective' test, the requirement to report will apply to you if based on the facts of the particular case, a person of your qualifications and experience would be expected to draw the conclusion that those facts should have led to a suspicion of money laundering. The main purpose of the objective test is to ensure that Jewellers (and other regulated persons) are not able to argue that they failed to report because they had no conscious awareness of the money laundering activity, for example by having turned a blind eye to incriminating information which was available to them, or by claiming that they simply did not realize that the activity concerned amounted to money laundering.

b) Attempted Transactions

You also have to pay attention to **suspicious attempted transactions**. If a customer attempts to conduct a transaction, but for whatever reason that transaction is not completed, and you think that the attempted transaction is suspicious, you must report it to the FIA.

Example of suspicious attempted transaction: a customer wants to purchase a $10,000 necklace, and to pay in cash, and you, as a Jeweler, ask for some identification from the customer who refuses to provide it. If you think that this cash is related to drug money or some other crime, you have to report that attempted transaction to the FIA. On the other hand, a customer simply asking how much the necklace costs would not be sufficient for it being an attempted transaction.

Therefore, an attempt is only when concrete action has been taken to proceed with the transaction.

NOTE: It is only when you know or reasonably suspect that the funds are criminal proceeds or related to money laundering or financing of terrorism that you have to report: you do not have to know what the underlying criminal activity is or whether illegal activities occurred.

C) How to Identify a Suspicious Transaction/Activity

You are the one to determine whether a transaction or activity is suspicious based on your knowledge of the customer and of the industry. You are better positioned to have a sense of particular transactions which appear to lack justification or cannot be rationalized as falling within the usual parameters of legitimate business. You will need to consider factors such as; is the transaction normal for that particular customer or is it a transaction which is a typical i.e. unusual; and the payment methods. Industry-specific indicators would also help you and your employees to better identify suspicious transactions whether completed or attempted.

NOTE: A list of red flags has been provided under clause 6 to guide you on identifying suspicious transactions.

5.3. Reporting Terrorist Funds

In accordance with regulation 12(7) and (8) of the Anti-Terrorism Regulations 2016, DPMS **must report immediately** to the FIA the existence of funds within your business where you know or have reasonable grounds to suspect that the funds belong to an individual or legal entity who:

- commits terrorist acts or participates in or facilitates the commission of terrorist acts or the financing of terrorism; or
- is a designated entity.

You **must report immediately** to the FIA where you know or have reasonable grounds to believe that a person or entity named on the UNSC sanctions' list or the list circulated by the FIA, has funds in Uganda.

You can access the UNSC Sanctions' list **("the UN list")** by visiting the United Nations website.

5.4. Reporting Cash Transactions

By virtue of section 8 of the AMLA, DPMS are required to report all cash and monetary transactions equivalent to or exceeding one thousand currency points.

5.5. Undertake Customer Due Diligence (CDD) Measures

In accordance with section 6 of the AMLA, DPMS are required to conduct CDD when the dealer engages in any cash transaction with a customer of high risk or in any foreign currency equivalent to or above United States Dollars 10,000. These cash transactions include domestic gemstone/jewellery sale or purchase, gemstones/jewellery imports or exports and, gemstone/jewellery sale or purchase using auctions and exhibitions.

CDD in general will be conducted as a minimum requirement. However, when it comes to situations where a customer is identified as of high risk with respect to ML and TF, the reporting entity should apply enhanced due diligence measures.

DPMS should ensure that they have in place a process for screening existing and prospective business relationships and customers against Sanctions Lists (see clause 5.2 and 5.3 above), and for performing background checks on them to identify any potentially adverse information (including associations with Politically Exposed Persons - 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.

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.

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.

DPMS should 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 PEPs, especially in regard to foreign customers.

Customer due diligence (CDD) measures as defined in section 6(3) of the Anti-Money Laundering Act as amended include but are not limited to:

- verify the identity of the client using reliable, independent source documents, data or information;
- identify and take reasonable measures to verify the identity of a beneficial owner;
- understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship to permit the accountable person to fulfil its obligations under the Act;
- if another person is acting on behalf of the customer, identify and verify the identity of that other person, and verify that person's authority to act on behalf of the customer;
- verify the identity of a customer using reliable, independent source documents, data or information, such as passports, birth certificates, driver's licences, identity cards, national identification card, utility bills, bank statements, partnership contracts and incorporation papers or other identification documents;
- verify the identity of the beneficial owner of the account, in the case of legal persons and other arrangements;
- conduct ongoing due diligence on all business relationships and scrutinise transactions undertaken throughout the course of the business relationship to ensure that the transactions are consistent with the accountable person's knowledge of the customer and the risk and business profile of the customer, and where necessary, the source of funds.

High Risk Customers/ Transactions

There are customers and types of transactions, services and products which may pose higher risk to your business and you are required to apply additional measures in those cases. The AML/CFT laws have identified certain high risk customers and require you to conduct enhanced due diligence ("EDD") on these

customers. You may also determine that certain customers', transactions and products pose a higher risk to your business and apply EDD.

You must apply EDD measures to high risk customers, which include, but are not limited to:

- obtaining further information that may assist in establishing the identity of the person or entity;
- applying extra measures to verify any documents supplied;
- obtaining senior management approval for the new business relationship or transaction sought by the person or customer;
- establishing the source of funds of the person or entity;
- carrying out on-going monitoring of the business relationship.

The enhanced due diligence measures shall be applied at each stage of the customer due diligence process and shall continue to be applied on an on-going basis.

5.6. Record Keeping

As per section 7 of the AMLA, DPMS are required to keep a record of each and every transaction for a specified period. Record keeping is important to anti-money laundering investigation which allows for swift reconstruction of individual transactions and provides evidence for prosecution of money laundering and other criminal activities.

DPMS must keep records in electronic or written form for a period of ten (10) years or such longer period as the FIA may direct. The records must also be kept for ten (10) years after the end of the business relationship or completion of a one-off transaction. The records to be kept are;

a) All domestic and international transaction records;
b) Source of funds declarations;
c) Customer's identification records;
d) Customer's information records;
e) Copies of official corporate records;
f) Copies of Suspicious Transaction Reports submitted by your staff to your anti-money laundering control officer;
g) A register of copies of suspicious transaction reports submitted to the FIA;
h) A register of all enquiries made by LEAs (date, nature of enquiry, name of officer, agency and powers being exercised) or other competent authority;
i) The names, addresses, position titles and other official information pertaining to your staff;
j) All wire transfer records; (originator and recipient identification data); and
k) Other relevant records.

5.7. Ascertain whether the customer is acting for a Third Party

In accordance with section 6(20) of the AMLA and regulation 16 of the AML Regulations, DPMS must take reasonable measures to determine whether the customer is acting on behalf of a third party especially where you have to conduct enhanced due diligence.

Such cases will include where the customer is an agent of the third party who is the beneficiary and who is providing the funds for the transaction. In cases where a third party is involved, you must obtain information on the identity of the third party and their relationship with the customer.

In deciding who the beneficial owner is in relation to a customer who is not a private individual (e.g., a company), you should identify those who have ultimate control over the business and the company's assets such as the

shareholders. Particular care should be taken to ensure that any person purporting to act on behalf of the company is fully authorized to do so.

5.8. Internal Control Measures

In accordance with regulation 11 of the AML Regulations, DPMS should develop, adopt and implement internal control measures, policies and procedures for the prevention of money laundering and financing of terrorism.

DPMS must take appropriate measures to ensure that all officers, employees, and agents engaged in dealing with clients or processing business transactions understand and comply with all applicable AML/CFT procedures.

DPMS must appoint a money laundering control officer (MLCO) with overall responsibility for AML/CFT compliance.

The MLCO must be in a senior managerial position and possesses sufficient professional experience and competence in the legal profession. The MLCO acts as the liaison point with the FIA and relevant supervisory authorities in Uganda, and commands the necessary independence and authority to train and supervise all other officers, employees, and agents within the firm.

The MLCO should at all times be resident in Uganda. In addition, it is highly recommended that an alternate to the MLCO is appointed to assume the prescribed responsibilities and duties in the MLCO's absence.

The MLCO's specific responsibilities include:

- establishing and maintaining a manual of compliance procedures;
- establishing an audit function to test AML/CFT procedures and systems;
- taking overall responsibility for all STRs; and

- ensuring that all officers, employees, and agents:
    - are screened by the MLCO and other appropriate officers before recruitment;
    - are trained to recognize suspicious transactions and trends and particular risks associated with money laundering and financing of terrorism; and
    - comply with all relevant obligations under AML/CFT laws and with the internal compliance manual.

MLCOs and reporting entities should review their arrangements on a regular basis, both to verify compliance with internal procedures and to ensure that those procedures are updated in light of any amendments to the AML/CFT legislation.

These guidelines do not specify the nature, timing, or content of the training that must be provided. This is a matter that must be addressed by the MLCO.

5.9. No Tipping Off

When you have made a suspicious transaction report to the FIA, you or your agent, employee must not disclose that you have made such a report or the content of such report to any person including the customer. According to section 117 of the AMLA, it is an offence to deliberately tell any person, including the customer, that you have or your business has filed a suspicious transaction report about the customer's activities/transactions. You must also not disclose to anyone any matter which may prejudice money laundering or financing of terrorism investigation or proposed investigation.

The prohibition applies to any person acting, or purporting to act, on behalf of a DPMS, including any agent, employee, partner, director or other officer, or any person engaged under a contract for services.

6. ML/TF INDICATORS (RED FLAGS) SPECIFIC TO DPMS

- Customer indiscriminately purchases merchandise without regard for value, size, or colour.
- A customer paying for high-priced jewellery with cash only but not in other popular and safe methods of payment. (e.g., credit card, debit card certified cheque).
- Unusual buying behaviour/pattern (e.g., repeated purchases of luxury products without apparent reasons).
- Purchases or sales that are unusual for the customer or supplier.
- Unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveler's checks, or cashier's cheques, or payment received from third-parties.
- Attempts by customer or supplier to maintain high degree of secrecy with respect to the transaction, such as request that normal business records not be kept.
- Customer is reluctant to provide adequate identification information when making a purchase.
- A customer orders item, pays for them in cash, cancels the order and then receives a large refund.
- A customer asking about the possibility of returning goods and obtaining a cheque (especially if the customer requests that cheque be written to a third party).
- Customer may attempt to use a third party cheque or a third party credit card.
- Funds come from an offshore financial centre rather than a local bank.

- Large or frequent payments made in funds.
- Transaction lacks business sense.
- Customer is known to have a criminal background.
- Customer uses or produces identification documents with different names.
- Customer does not want to put his/her name on any document that would connect him/her with the purchase.
- Purchase appears to be beyond the means of the customer based on his/her stated or known occupation or income.
- Person pawns numerous items at the same time.
- Persons pawn items repeatedly.
- Persons pawn items with price tags on them.
- Person cannot explain the provenance of the items they seek to pawn.
- It is important to note that it is not only cash transactions that may be suspicious.
- Cash payment is only mentioned by the customer at the conclusion of transaction.
- Instruction on the form of payment changes suddenly just before the transaction goes through.
- A cash transaction is unusually large.
- The customer will not disclose the source of the cash.
- The explanation by the business and/or the amounts involved is not credible.
- The customer is buying from an unusual location in comparison to their locations.
- A series of transactions are structured just below the regulatory threshold for due diligence identity checks.
- The method of delivery is unusual, for example, a request for immediate delivery, delivery to an address other than the customers address or the loading of high volume/ bulky goods immediately into the customers own transport.

- Unnecessary routing of funds through third parties.
- Enquiries about the business's refund policy.
- Transactions that appear to be structured to avoid reporting requirements.
- Customer may attempt to use a third-party cheque or a third-party credit card.
- Transaction lacks business sense.
- Purchases or sales that are not in conformity with standard industry practice. For example, one money-laundering scheme observed in this industry involved a customer who ordered items, paid for them in cash, cancelled the order, and then received a large refund.

7. PENALTIES FOR NON-COMPLIANCE

Failure to comply with the obligations under the AMLA and the AML regulations may result in criminal and/or administrative sanctions.

Penalties may include fines and terms of imprisonment. Sanctions include possible revocation of licenses, issuance of directives and court orders.

The offences under the AMLA include;

a. Money Laundering (section 3 and 116);
b. Tipping Off (section 117);
c. Falsification, Concealment of documents (section 118);
d. Failure to identify persons (section 119);
e. Failure to keep records (section 120);
f. Facilitating money laundering (section 121);
g. Destroying or tampering with records (section 122);
h. Refusal, omission, neglect or failure to give assistance (section 123);
i. Failure to report cash transactions (section 124);
j. Failure to report suspicious or unusual transactions (section 125);

k. Failure to report conveyance of cash into or out of Uganda (section 126);
l. Failure to send a report to the Authority (section 127);
m. Failure to comply with orders made under the Act (section 128);
n. Contravening a restraining order (section 129);
o. Misuse of information (section 130);
p. Obstructing an official in performance of functions (section 131);
q. Influencing testimony (section 132);
r. General non-compliance with requirements of this Act and conducting transactions to avoid reporting duties (section 133);
s. Unauthorised access to computer system or application or data (section 134);
t. Unauthorised modification of contents of computer system (section 135).

Penalties

According to section 136 of the AMLA, a person who commits money laundering is liable on conviction to:-

a. in the case of a natural person, imprisonment for a period not exceeding fifteen years or a fine not exceeding one hundred thousand currency points or both;
b. in the case of a legal person by a fine not exceeding two hundred thousand currency points.

According to section 136(2) of the AMLA, a person who commits any other offence under the Act is punishable-

a. if committed by a natural person, by imprisonment for a period not exceeding five years or a fine not exceeding thirty three thousand currency points, or both;
b. if committed by a legal person such as a corporation, by a fine not exceeding seventy thousand currency points;

c. if a continuing offence, by a fine not exceeding five thousand currency points for each day on which the offence continues; or
d. if no specific penalty is provided, by a fine not exceeding nine thousand currency points and in case of a continuing offence, to an additional fine not exceeding five thousand currency points for each day on which the offence continues

8. REVIEW OF THE GUIDELINES

DPMS are encouraged to compile and record any comments, which arise in relation to these guidelines, and forward them to the Financial Intelligence Authority for its appropriate action.

Sydney Asubo
Executive Director
Financial Intelligence Authority