Suspicious Transaction Reporting Guidelines

Precious Stones and Metals Sector

1.0 INTRODUCTION

In keeping with international obligations and ensuring that Zambia's financial institutions and other non-financial businesses and professions are not abused by persons involved in money laundering (ML) or the financing of terrorism (TF) , the Financial Intelligence Centre ('the FIC ') was established to receive suspicious transaction reports (STRs) from reporting entities, analyze and disseminate intelligence to law enforcement agencies (LEAs), pursuant to the Financial Intelligence Centre Act No 46 of 2010 ('the Act')(as amended).

It is the responsibility of the FIC to issue guidelines to reporting entities to ensure reporting entities comply accordingly with the provisions of the Act. The purpose of these guidelines is to provide industry specific guidance for dealers in precious stones and metals on their legal obligations for measures to deter and detect money laundering and financing of terrorism activities and to assist the reporting entities to comply with the Act.

These STRs Guidelines have been issued in accordance with section 56 and pursuant to section 29 of the Act. One of the cardinal responsibilities of reporting entities is to submit a suspicious transaction report where there is suspicion that a transaction may arise from the commission of a crime or may be linked to the financing of terrorism.

1.1 Overview of the Precious Stones and Metals Sector

The Financial Action Task Force (FATF), the body which sets standards internationally for money laundering and financing of terrorism, in evaluating risks and vulnerable activities has found that money laundering and financing of terrorism activities have involved precious metals and precious stones. A dealer in precious metals and precious stones has been identified as a business which is vulnerable. FATF has acknowledged the vulnerability of dealers in precious stones and precious metals by recommending that such business activity should be subject to Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) requirements.

The risks of misusing the dealers in precious stones and metals are due to the fact that precious metals, particularly gold, attracts money launderers, as it has a high actual value and can be found in relatively small sizes, thus facilitating its transport, purchase and sale in several regions around the world.

Precious metals and stones, particularly gold and diamond, offer a high intrinsic value in a compact form. They can be "cashed" easily in most areas of the world. Hence, they are vulnerable to be used in money laundering for the ease in which they can be hidden and transported. For example, gemstones and diamonds in particular, maybe used as a way of storing terrorist assets outside the formal financial sector. The aim is no

longer only in turning a profit but also acquiring as many stones as possible with crime proceeds that are being kept out of banks and businesses.

Gold also preserves its value regardless of its form whether it comes in the form of bullions or golden articles. Dealers are often interested in gold more than gems as it may be melted to change its form while preserving its value.

Gold is used in ML operations whether it is acquired in an illicit manner (like theft or smuggling) where it constitutes proceeds of a crime and is therefore deemed to be an illicit fund, or is used as a ML means through the purchase of gold using funds.

Diamonds can also be traded around the world easily as the small size of diamond stones and their high value facilitate their concealment. In some cases, it was noted that diamonds are used as a means to finance terrorist acts and groups.

The Mines and Minerals Development Act No. 11 of 2015 provides the legislation covering exploration, mining and processing of minerals. Sections 44 to 45 of the Mines and Minerals Development Act No. 11 of 2015 requires traders (domestic or International) in minerals to obtain a permit from the Director of Mines which is valid for three (3) years.

Under section 5 of the FIC Act the Center is empowered to supervise sectors for AML where no specific supervisor is designated. In this regard, the Centre is the AML supervisory authority for the dealers in Metals and Precious Stones.

1.2 Scope of the Guidelines

The Precious Stones and Metals Sector STR guidelines have incorporated essential elements of the Act, relevant FATF-Recommendations and other international best practices on AML/CFT regime. These guidelines cover among others the following key areas of AML/CFT policy; Customer due diligence, the AML/CFT Compliance programme; monitoring and responding to suspicious transactions.

The STR Guidelines are provided as general information only and as such do not represent all the requirements under the law or the obligations imposed by the Ministry of Mines and Minerals Development. The guidelines do not constitute legal advice and are not intended to replace the Act or any other guidelines, directives or regulations issued by the Supervisory Authority.

2.0 DEFINITION OF KEY TERMS

Attempted Transaction: Is one where a customer intended to conduct a transaction and took some form of action to do so. It is different from a simple request for information, such as an enquiry as to the price of a certain item. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the customer.

Financial Action Task Force (FATF): Is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counterterrorist financing (CFT) standard.

Money Laundering: Under The Prohibition and Prevention of Money Laundering Act No 14 of 2001, as amended by Act No.44 of 2010, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means a serious offence as defined in the Forfeiture of Proceeds of Crime Act, No. 19 of 2010. It includes among others those relating to illegal drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation. A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Zambia.

Politically exposed Persons (PEPs): Are individuals who are or have been entrusted with prominent public functions both in Zambia and foreign countries and those associated with them.

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 semiprecious stones and man-made gemstones.

Reporting Entity: An institution regulated by a Supervisory Authority and required to make a suspicious transaction report on suspected Money Laundering, Terrorist Financing and other serious offences under the Act. In accordance with Section 2 of the Act, dealers in precious stones and metals are designated as Reporting Entities.

Terrorist Financing: Terrorist financing offences extend to any person who willfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part to carry out a terrorist act by a terrorist organization or an individual terrorist. Under the Anti-Terrorism Act No. 21 of 2007 as amended by Act No. 2 of 2015, it is an offence to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorism or terrorist financing activities.

3.0 CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) is the identification and verification of both the customer and beneficiary including but not limited to continuous monitoring of the business relationship with the reporting entity. Reporting Entities are not permitted to operate anonymous accounts or accounts in fictitious names.

Part III of the Act requires reporting entities to institute measures to ensure effective CDD at all times. Reporting Entities shall undertake measures when:

i. Establishing a business relationship with or conducting a business transaction for a customer

ii. Carrying out a transaction in an amount equal to, or above such amount as may be prescribed including where the transaction is carried out in a single operation or several operations that appear to be linked

iii. The Customer wishes to carry out a domestic or international wire transfer of monetary amounts in the amounts equal to, or above, the prescribed amount

iv. There is a suspicion of money laundering or terrorist financing

v. There are doubts about the veracity or adequacy of previously obtained customer identification data.

3.1 Customer Due Diligence Procedures

a. Reporting Entities shall identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable, independently sourced documents, such as a validly issued National Registration Card, Passport, Drivers' Licence, (which should not have expired at the time of conducting CDD) Certified Certificate of Incorporation or such other information as the Minister may prescribe.

b. In respect of customers that are legal persons or legal arrangements, reporting entities shall:

i. verify any person purporting to have been authorised to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person; and

ii. Verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from a recognised established body or similar evidence of establishment or existence and any other relevant information.

c. Reporting entities shall identify a beneficial-owner and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial-owner is.

d. Reporting entities shall in respect of all customers determine whether or not a customer is acting on behalf of another person.

Where the customer is acting on behalf of another person, the reporting entity shall take reasonable steps to obtain sufficient identification-data and to verify the identity of that other person.

e. Reporting entities shall take reasonable measures in respect of customers that are legal persons or legal arrangements to:

i. Understand the ownership and control structure of such a customer; and

ii. Determine the natural persons that ultimately own or control the customer. For trusts – The natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries.

f. Reporting entities shall obtain information on the purpose and intended nature of the business relationship of their potential customers.

g. Reporting entities shall conduct ongoing due diligence on the business relationship as stated by the customers above.

h. The ongoing due diligence above includes scrutinizing the transactions undertaken by the customer throughout the course of the financial institution/ customer relationship to ensure that the transactions being conducted are consistent with the reporting entities' knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).

i. Reporting entities shall ensure that documents, data or information collected under the CDD-process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of higher-risk business relationships or customer categories. All books and records with respect to its customers and transactions should be maintained for a period of at least 10 years;

3.2 High-Risk Categories of Customers

Reporting entities are required to have appropriate risk management systems to identify customers whose activities may pose a high risk of money laundering and financing terrorism. Reporting entities need to exercise enhanced identification, verification and ongoing due diligence procedures with respect to High Risk Customers. Reporting entities shall perform enhanced due diligence for high-risk categories of customers, business relationships or transactions. Examples of high-risk customer categories include:

a. Companies that have nominee-shareholders or shares in bearer form;

b. Non-resident customers;

c. Legal persons or legal arrangements such as trusts that are personal-assets holding vehicles;

d. Politically Exposed Persons (PEPs).

Reporting Entities shall, in addition to performing CDD procedures, put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial-owner is a PEP.

The risk management systems used by reporting entities to identify customers whose activities may pose a high risk of money laundering and financing of terrorism shall require:-

I. Enhanced identification-which involves identifying customers or activities engaged in by customers who may pose high risk of money laundering or financing of terrorism by taking into account:

a. the nature and business of customers;

b. customer activities, transaction patterns and operations;

c. geographic location of the customer and/or transaction

d. the magnitude of customer assets that a reporting entity handles;

e. third parties that may be involved in the customer's activities;

f. the beneficial ownership of an entity and their impact on risk;

g. volume of cash used by customer in their transactions; and

h. any other indicators that may be relevant.

II. Verification and on-going Due Diligence-which includes:

a. Seeking additional information beyond the minimum requirements under the law to substantiate the customer's identity or the beneficial ownership of an entity and

b. Obtaining additional information about the intended nature and value of a given transaction.

Reporting Entities shall obtain senior management approval before they establish a business relationship with PEP. Where a customer has been accepted or has an ongoing relationship with the reporting entity and the customer or beneficial-owner is subsequently found to be or becomes a PEP, the reporting entity shall obtain senior management approval in order to continue the business relationship. Reporting entities shall take reasonable measures to establish the source of wealth and the sources of funds of customers and beneficial-owners identified as PEPs and report all anomalies or unusual and abnormal transactions immediately to the Centre. Reporting Entities in business relationships with PEPs are required to conduct enhanced ongoing monitoring of that relationship.

4.0 THE ANTI-MONEY LAUNDERING (AML) AND COUNTERING THE FINANCING OF TERRORISM (CFT) COMPLIANCE PROGRAMME

An AML/CFT programme is an essential component of a reporting entity's compliance regime. The AML/CFT compliance programme should be risk based, and should be designed to mitigate the Money Laundering and Terrorist Financing risks the reporting entity may encounter.

4.1. Elements of an AML/CFT Programme

4.1.1 A system of internal policies, procedures and controls

Reporting Entities shall adopt policies indicating its commitment to comply with AML/CFT obligations under the relevant Acts and regulations to prevent any transaction that facilitates ML/TF activities. Every reporting entity shall formulate and implement internal rules procedures and other controls that will deter criminals from using its facilities for money laundering and terrorist financing and to ensure that its obligations under the relevant laws and regulations are always met. These procedures, policies and controls should cover the CDD, record retention, the detection of unusual and suspicious transactions, the reporting obligation, among other things.

4.1.2 Compliance Officer

Reporting Entities should designate a Compliance Officer within its organisation who shall receive suspicious or unusual transaction reports from persons handling transactions within the entity. Each Compliance Officer shall be equipped with the relevant competence, authority and independence to implement the institution's AML/CFT compliance programme. The Compliance Officer shall have ready access to all the books, records and employees of the reporting entity necessary to fulfil the responsibilities under the Act.

An employee of a reporting entity shall promptly report to a designated Compliance Officer all cases where: a) the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that a customer has been or is involved in an illegal activity or crime; or b) a customer in respect of whom the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that another customer has been engaging in illegal activities or crimes.

The duties of the Compliance Officer shall include but shall not be limited to the following:

i. Developing an AML/CFT Compliance Programme;
ii. Receiving and vetting suspicious transaction reports from staff;
iii. Filing suspicious transaction reports with the Centre;
iv. Ensuring that the reporting entities' compliance programme is implemented;
v. Co-ordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements; and
vi. Serving both as a liaison officer with the FIC as well as a point-of-contact for all employees on issues relating to money laundering and terrorist financing. Every reporting entity shall ensure that the Compliance Officer has access to other information that may be of assistance to the anti-money laundering reporting officer in consideration of a suspicious or unusual transaction.

A reporting entity shall cooperate with the Law enforcement Agencies to facilitate the exchange of information relating to money laundering and terrorist financing.

4.1.3 Training

The Act requires reporting entities to have formal, written AML/CFT Compliance programmes that include training. Ongoing employee training programs should be in place in all reporting entities to ensure that employees are kept informed of new developments, including information on current ML and FT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction

reporting. The timing, coverage and content of the employee training program should be tailored to meet the perceived needs of the reporting entity.

4.1.4 Independent Audit

Putting your AML/CFT Compliance programme in place is not enough. The programme must be monitored and evaluated.

Therefore, reporting entities are supposed to have an independent audit performed by people not involved with the entity's AML/CFT Compliance staff to test compliance with the procedures, policies and controls. The individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors.

Monitoring of AML/CFT Compliance programme

The FIC will from time to time undertake on and off-site inspections to reporting entities to monitor how the AML/CFT Compliance programmes are being implemented.

I. Obligation to Report Suspicious Transaction

Whenever a reporting entity processes a transaction to which there is reasonable grounds to suspect that any property is the proceeds of crime, or is related to, or is to be used for, terrorism, terrorist acts or by terrorist organisations or persons who finance terrorism, it should take reasonable measures to ascertain the purpose of that transaction and submit a report to the Centre, setting out the suspicion, within three (3) working days of forming that suspicion.

Further, a reporting entity is required to exercise caution when carrying out a transaction which it suspects to be related to money laundering or financing of terrorism. The Act also requires an STR to be submitted on attempted money laundering or financing of terrorism.

In exceptional cases (transactions that require immediate action), making a suspicious transaction report to the FIC does not prevent a reporting entity from reporting suspicions of money laundering or financing of terrorism directly to law enforcement agencies. Nevertheless, an STR still need to be submitted to the FIC. The FIC encourages reporting entities to maintain established relationships with law enforcement agencies.

Failure to submit a suspicious transaction report to the FIC may lead to imprisonment upon conviction to a term of up to seven years or payment of a fine of seven hundred thousand penalty units or to both.

II. Prohibition against Tipping Off

A reporting entity or any director, partner, officer, principal or employee of the reporting entity is not allowed to disclose to any person the contents of the STR Form. Further, the disclosure of any other information from which a person could reasonably be expected to conclude that a suspicion has been formed or that a report has been or may be made is prohibited.

Any person who contravenes this requirement commits an offence and is liable to a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

III. Protection of identity of persons and information relating to STRs

A reporting entity is not allowed to disclose any information that identifies, or is likely to identify the person who prepared or made a suspicious transaction report, or handled the underlying transaction. In light of the foregoing, the disclosure of identity of the above mentioned person is confidential. Section 47 of Act prohibits the disclosure of confidential information. Such disclosure is an offence which may result in a fine of up to five hundred thousand penalty units or to imprisonment for a period not exceeding five years, or to both.

IV. Protection of entities/persons reporting

No civil, criminal, administrative or disciplinary proceedings for breach of banking or professional secrecy or contract shall be taken against you for submitting a completed STR Form, in good faith, or in compliance with directions given by the Act.

5.0 HOW TO IDENTIFY A SUSPICIOUS TRANSACTION IN THE PRECIOUS STONES & METALS SECTOR

Where there is a business relationship, a suspicious transaction will often be one which is inconsistent with your customer's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is knowing enough about your customer and customer's business, to recognize that a transaction or series of transactions are unusual.

Reliance on what should be reported is largely on one's assessment, based on knowledge and experience, as well as specific circumstances of the transaction. The assessment should therefore be based on a reasonable evaluation of relevant factors, including the knowledge of the clients business, financial history, background and behavior.

5.1. Specific Money Laundering/Terrorist Financing Indicators in the Precious Stones and Metals Sector

As entities and personnel working in the precious stones and minerals sector, there is need to note that there are numerous indicators which may assist you to identify potential money laundering or terrorism financing activities. Although the existence of a single indicator does not necessarily indicate illicit activity, it should encourage further monitoring and examination.

In most cases, it is the existence of multiple indicators which raises a reporting entity's suspicion of potential criminal activity, and informs their response to the situation. Directors and Senior Management should include these money laundering/terrorism financing indicators in staff training and encourage their staff to use these indicators when describing suspicious behaviours for inclusion in suspicious matter reports submitted to the Centre.

ML/TF indicators for the Precious Stones and Metals Sector

The list below features some of the major indicators of money laundering and terrorist financing in the Precious Stones and Metals Sector and should be treated as a non exhaustive guide:

The following red flags should be considered wen buying or selling Precious Stones and Metals:

i. Customer indiscriminately purchases merchandise without regard for value, size, or colour.
ii. 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)
iii. Unusual buying behaviour/pattern (e.g., repeated purchases of luxury products without apparent reasons
iv. Purchases or sales that are unusual for the customer or supplier.
v. Unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveller's checks, or cashier's cheques, or payment received from third-parties.
vi. 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.
vii. Customer is reluctant to provide adequate identification information when making a purchase.

viii. A customer orders item, pays for them in cash, cancels the order and then receives a large refund.
ix. 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).
x. Customer may attempt to use a third party cheque or a third party credit card.
xi. Funds come from an offshore financial centre rather than a local bank.
xii. Large or frequent payments made in funds other than TT dollars.
xiii. Transaction lacks business sense.
xiv. Customer is known to have a criminal background.
xv. Customer uses or produces identification documents with different names.
xvi. Customer does not want to put his/her name on any document that would connect him/her with the purchase.
xvii. Purchase appears to be beyond the means of the Customer based on his/her stated or known occupation or income.

6.0 HOW TO OBTAIN SUSPICIOUS TRANSACTION FORMS

You may obtain the STR forms by contacting the FIC office using the address provided under paragraph nine (9) of this document or emailing fic@ficzambia.gov.zm. Further, an electronic copy of the STR form can be accessed on the FIC website (www.fic.gov.zm).

7.0 HOW TO COMPLETE A SUSPICIOUS TRANSACTION REPORT

When completing an STR form, you MUST follow the instructions contained in the form and ensure that mandatory fields are duly completed.

8.0 HOW TO SEND YOUR SUSPICIOUS TRANSACTION REPORTS TO FIC

The completed STR form by confidential cover, must be reported through the following means:

i. On the FIC e-system (applicable only to reporting institutions with electronic link with the FIC);
ii. Authenticated FIC email address provided for under six (6) of this document;
iii. Registered courier service providers using the address provided for in paragraph nine (9) below; and
iv. To be hand delivered to designated officials of the Monitoring and Analysis Department of the Centre premises.

9.0 FINANCIAL INTELLIGENCE CENTRE CONTACT DETAILS

All the completed reports or any queries should be sent to:

The Director General Financial Intelligence Centre

Plot 50 L, Kudu Road, Kabulonga

P O Box 30481

Lusaka

ZAMBIA