



GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO



FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO

Ministry of Finance

**AML/CFT/CPF GUIDANCE FOR JEWELLERS
LICENSED UNDER THE LICENSING OF DEALERS
(PRECIOUS METALS AND STONES) ACT UPDATED 11
APRIL 2024**

Purpose

This Guidance is intended to provide assistance to persons engaged in the business of Jewellery licensed under the Licensing of Dealers (Precious Metals and Stones) Act in Trinidad and Tobago with their AML/CFT/CPF obligations.

Table of Contents

1. INTRODUCTION.....	3
2. WHY SUPERVISE JEWELLERS?	4
3. DO THESE OBLIGATIONS APPLY TO YOU?.....	6
4. WHAT ARE YOUR AML/CFT/CPF LEGAL OBLIGATIONS?	7
I. REGISTRATION WITH THE FIUTT	7
• Change of address or change of Directors.....	7
• De-registration	8
II. APPOINT A COMPLIANCE OFFICER AND ALTERNATE COMPLIANCE OFFICER	9
III. ASSESSING ML/FT/PF RISK	9
IV. DEVELOP AND IMPLEMENT A COMPLIANCE PROGRAMME	12
V. CONDUCTING CUSTOMER DUE DILIGENCE	12
VI. TRAINING	13
VII. INTERNAL AND EXTERNAL AUDIT	13
VIII. SUBMISSION OF REPORTS TO THE FIUTT.....	14
• Reporting Suspicious Transactions and Activities.....	14
• Reporting Terrorist Property/Funds	14
• Reporting Property/Funds for the Proliferation Financing of weapons of mass destruction. ...	15
IX. RECORD KEEPING	17
5. GENERAL OFFENCE FOR FAILURE TO COMPLY WITH THE REGULATIONS AND FORS.....	17
APPENDIX 1 - CASE STUDIES	19

1. INTRODUCTION

This Guidance is intended to provide assistance to persons or entities, engaged in the business of Jewellery licensed under the Licensing of Dealers (Precious Metals and Stones) Act and supervised by the Financial Intelligence Unit of Trinidad and Tobago (the FIUTT), in complying with their Anti-Money Laundering, Counter Financing of Terrorism and Counter Proliferation Financing (“AML/CFT/CPF”) legal obligations.

In accordance with the Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01 (“FIUTTA”) and the Proceeds of Crime Act, Chap. 11:27 (“POCA”) the FIUTT is the Supervisory Authority for all listed businesses. These listed businesses are itemised in the First Schedule of the POCA, within which Jewellers licensed under the Licensing of Dealers (Precious Metals and Stones) Act, Chapter 84:06, are included.

Every individual or entity conducting the business of jewellery, as described in the First Schedule of the POCA, is required to honour his/its AML/CFT/CPF obligations set out in the following Acts and Regulations:

1. The Financial Intelligence Unit of Trinidad and Tobago Act, Chapter 72:01 (“FIUTTA”)
2. The Financial Intelligence Unit of Trinidad and Tobago regulations, 2011 (“FIUTT Regulations”)
3. The Proceeds of Crime Act, Chapter 11:27 (“POCA”)
4. The Financial Obligations Regulations, 2010 (“FORs”)
5. The Anti-Terrorism Act, Chapter 12:07 (“ATA”)
6. The Financial Obligations (Financing of Terrorism) Regulations, 2011 (“FOFTRs”)
7. Economic Sanctions (Implementation of United Nations Resolutions on the Democratic People’s Republic of Korea) Order, 2018 (“ESO”)
8. Economic Sanctions (Implementation of United Nations Resolutions on the Islamic Republic of Iran) Order, 2023 (“ESO”)

N.B. This Guidance is a general, informative document and is not intended to replace any of the above mentioned AML/CFT/CPF Acts and Regulations. This Guidance should not be construed as legal advice and should be read in conjunction with the said laws.

[Intentionally left blank]

2. WHY SUPERVISE JEWELLERS?

Jewellery is a Listed Business described in the First Schedule of the POCA as ***‘a Business licensed under the Licensing of Dealers (Precious Metals and Stones) Act’***. Entities and individuals who engage in this activity as a business may be vulnerable to abuse by criminals seeking to launder the proceeds of crime or finance illegal activities. This vulnerability can be attributed to the fact that gold, diamonds and other precious metals and stones are high in value and can easily be used to convert large amounts of illicitly obtained cash through its purchase.

FATF in its guidance, [“Money laundering/terrorist financing risks and vulnerabilities associated with gold”](#)¹, highlighted that gold, in particular, is highly attractive to criminal syndicates wishing to hide, move or invest their illicit proceeds given that the market is highly reliant on cash as the method of exchange and that the properties of gold make tracking its origins very difficult. Cash-for-gold businesses have the potential to provide criminal groups with a continuous supply of untraceable gold commodities from various sources.

Further, gold is a potentially attractive vehicle for money laundering because it can be easily transported, it is universally accepted, it provides anonymity, it is easily converted and can be sold at market value for purposes of reintegrating funds without attracting authorities. As such, criminals may launder cash or other payment means acquired through predicate offences he commits by placing and layering through the purchase of precious metals e.g. diamonds and gold trade.

As it relates to terrorist financing, diamonds, as well as other precious metals and stones, can be used to finance terrorism in a scenario where a donor or financier purchases diamonds legitimately, using lawfully derived funds, and then transfers the diamonds to a terrorist or terrorist organisation who use the diamonds in exchange for equipment or cash intending to finance terrorist activities².

FATF also highlighted in its Guidance on Proliferation Financing Risk Assessment and Mitigation, dated June 2021³, that typologies have revealed how dealers in precious metals and stones face exploitation by designated persons and entities, or those acting on their behalf or under their control, for the purposes of effecting a potential breach, non-implementation or evasion of Proliferation financing related targeted sanctions the sector provides an alternative method for designated persons and entities to surreptitiously move financial resources across international borders.

¹ FATF and APG (2015), Money laundering and terrorist financing risks and vulnerabilities associated with gold, FATF, Paris and APG, Sydney

www.fatf-gafi.org/topics/methodsandtrends/documents/ml-tf-risks-and-vulnerabilities-gold.html

² FATF Report MONEY LAUNDERING AND TERRORIST FINANCING THROUGH TRADE IN DIAMONDS October 2013:

<https://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf>

³ FATF (2021), Guidance on Proliferation Financing Risk Assessment and Mitigation, FATF, Paris, France,

<https://www.fatf-gafi.org/publications/financingofproliferation/documents/proliferation-financing-riskassessment-mitigation.html>

Accordingly, Jewellers may unwittingly be misused by criminals for Money Laundering, Terrorist Financing, Proliferation Financing (“ML/TF/PF”). It is vital therefore that Jewellers be aware of their ML/TF/PF and illicit trade risks and adopt the right measures to mitigate these risks.

The requirement for Jewellers to register with the FIUTT and comply with AML/CFT/CPF obligations enables them to effectively mitigate these risks and ultimately avoid potential misuse.

For scenarios demonstrating the misuse of Jewellers for money laundering, please see [Appendix 1](#)

Please see the FIUTT’s [Advisory to Jewellers and Financial Institutions: The Purchase of Jewellery/Gold Relative to Money Laundering](#) to understand further ***the process by which Jewellers may be misused.***

[Intentionally left blank]

3. DO THESE OBLIGATIONS APPLY TO YOU?

These obligations apply to you if you are an individual or company, partnership or firm licensed under the Licensing of Dealers (Precious Metals and Stone) Act to conduct the business of jewellery (a “Jeweller”).

Please note that Section 3 of the Licensing of Dealers (Precious Metals and Stones) Act requires you to obtain a license, as prescribed therein, in order to carry on the business of a dealer in precious metals and stones.

It should be noted that “precious metals” include bullion, platinum, gold and silver coins, and jewellery made from same and “stones” include diamonds, rubies and precious and semiprecious stones⁴.

[Intentionally left blank]

⁴ Section 2 Licensing of Dealers (Precious Metals and Stones) Act, Chapter 86:04

4. WHAT ARE YOUR AML/CFT/CPF LEGAL OBLIGATIONS?

The AML/CFT/CPF laws of Trinidad and Tobago impose the following obligations:

- I. [Registration with the FIUTT](#)
- II. [Appoint a Compliance Officer and Alternate Compliance Officer](#)
- III. [Assessing ML/FT/PF Risks](#)
- IV. [Develop and implement a Compliance Programme](#)
- V. [Conducting Customer Due Diligence](#)
- VI. [Training](#)
- VII. [Internal and External Audits](#)
- VIII. [Submission of Reports to the FIUTT](#)
- IX. [Keep Records](#)

Please note that this is not an exhaustive list of obligations and each entity is required to consult the AML/CFT/CPF laws referred to at the Introduction of this Guidance to ensure compliance.

I. REGISTRATION WITH THE FIUTT

You **must** register with the FIUTT if you are a Jeweller as explained at [section 3](#) herein. Your application for registration must be received within three months of commencing this business activity or of your incorporation as a company or registration as a business under the laws of Trinidad and Tobago, whichever is the **earlier** date. *(See Section 18B of the FIUTTA and Regulation 28(1) of the FIUTT Regulations).*

To register with the FIUTT, you may visit the FIUTT's website to access the [FIUTT Registration of Supervised Entities Form](#) and [relevant instructions](#).

Please note that pursuant to Regulation 28(2) of the FIUTT Regulations, failure to register with the FIUTT within the time stipulated is an offence for which you are liable on summary conviction to a fine of \$50,000 and to a further fine of \$5,000 for each day the offence continues.

- Change of address or change of Directors

You are required to notify the FIUTT where there is a change of Directors, Owners, Partners or Compliance Officer within thirty (30) days of such change.

You must also notify the FIUTT of a change of address of your registered office or principal place of business within thirty (30) days of such change. *(See Regulations 29(1) and 29A of the FIUTT Regulations)*

Jewellers supervised by the FIUTT are required to complete the Compliance Officer Fit and Proper Questionnaire, where there is a change of the Compliance Officer and Alternate Compliance Officer.

Submissions of such changes can be made manually or electronically.

To make a manual submission, visit the FIUTT at Level 25, Tower D, International Waterfront Complex, 1A Wrightson Road. Electronic submissions can be made via email to fiucompliance@gov.tt

Failure to notify the FIUTT of a change of address of your registered office or principal place of business within thirty (30) days is an offence and you are liable on summary conviction to a fine of twenty thousand dollars (\$20,000).

Additionally, failure to notify the FIUTT of a change of Directors, Owners, Partners or Compliance Officer within thirty (30) days is an offence and you will be liable on summary conviction to a fine of twenty thousand dollars \$20,000. (See Regulations 29(2) and 29A (2) of the FIUTT Regulations).

- **De-registration**

In the circumstances where your entity *no longer holds a valid license* granted pursuant to the Licensing of Dealers (Precious Metals and Stones) Act **and no longer intends to perform** the business activities of a Jeweller, it is advised that an application for de-registration is made to the FIUTT (See Section 18BA of the FIUTTA). In order to deregister with the FIUTT, you must first ensure that your business is **not** engaged in **any** business activity listed on the FIUTT's **List of Supervised Sectors**.

To deregister with the FIUTT, you must submit:

- ✓ a completed Deregistration Form to the FIUTT ([click here to access the De-registration of Listed Business Form](#)); and
- ✓ evidence that you are no longer performing the activities which required you to be registered with the FIUTT.

Such evidence may include, in the case of a Company, your letter of request to the Registrar General's Department to be struck off the Companies Registry, or, request for an amendment to the nature of business on your Articles of Incorporation.

In the case of a Registered Business, you are required to submit copy of your Notice of Cessation (Form 9), as the legal presumption is that the business is being carried on, as long as the business name remains on the Register of Business Names⁵. Submissions for deregistration can be made manually or electronically. To make a manual submission, visit

⁵ See guidance from the Registrar General's Department under the heading "Businesses Registered Under the Registration of Business Names Act Chap. 82:85" at the following link: <http://legalaffairs.gov.tt/faqs.php>.

the FIUTT at Level 25, Tower D, International Waterfront Complex, 1A Wrightson Road. Electronic submissions can be made via email to fiucompliance@gov.tt.

Once the FIUTT is satisfied that **you no longer hold a valid license granted under the Licensing of Dealers (Precious Metals and Stones) Act AND that you no longer intend on performing the activities of a Jeweller**, your application for deregistration will be accepted and you will be issued with a Notice of De-registration. In addition, your entity's name will be removed from the FIUTT's List of Registrants, inserted to the FIUTT's List of De-Registration, and uploaded on our website.

II. APPOINT A COMPLIANCE OFFICER AND ALTERNATE COMPLIANCE OFFICER

Regulation 3(5) of the FORs requires you to designate a Compliance Officer for the purpose of securing compliance with AML/CFT/CPF obligations. Regulation 3(8) of the FORs requires you to also appoint an alternate compliance officer who will be required to undertake the functions of the Compliance Officer should the Compliance Officer be absent from duty for both short and extended periods of time.

In accordance with Regulations 3(6) of the FORs, the Compliance Officer and alternate Compliance Officer of the business shall be a senior employee of the business or such other competent professional.

Please note that Regulations 3(8) and 3(10) of the FORS mandates that you seek the written approval of the FIUTT after designating persons as the business' Compliance Officer and Alternate Compliance Officer, respectively.

For guidance on designating a Compliance Officer and Alternate Compliance Officer, and receiving approval from the FIUTT, please [click here](#).

III. ASSESSING ML/FT/PF RISK

Regulation 7 of the FORs requires you to adopt a risk-based approach to monitoring financial activities within your business. Essentially, you are required to take steps to identify, assess, understand and document the ML/FT/PF risks of your business to determine those clients/transactions that are of low, medium or high risk.

FATF advises in its guidance, updated July 2022, that a risk assessment will aid in identifying the ML/TF/PF risks that your business is potentially exposed to during the course of its activities. Further, a documented assessment should include current and emerging ML/TF/PF trends while considering how such issues may impact the business.

Your risk assessment ought to follow an approach that considers, amongst other things, the size of your business, the financial value of transactions involving your business and the nature of such transactions

When identifying potential risks to your business, the primary risk categories may include:

1. **Country or Geographic risk** - this includes noting the country/jurisdiction where your customers, parties to the transactions and/or the property involved, are from. You must consider the effectiveness of that country's AML/CFT/CPF regime, identified deficiencies, whether the country is subject to sanctions by international organisations. This can be done through conducting checks on the FATF's list of High Risk Jurisdictions subject to a Call for Action and jurisdictions under increased monitoring. The FIUTT regularly publishes FATF public statements of jurisdictions who have been added to and removed from these lists [here](#).

Country or Geographic risk should also be considered when the funds to be used in the transaction have been generated from abroad and the transaction is conducted without face-to face contact.

2. **Customer risk**- this includes considering the degree of ML/TF/PF risk posed by your customer and the parties involved in the transaction including any beneficial owners.

Higher risk circumstances for customers include, but are not limited to, whether the parties are from a higher risk jurisdiction, as identified above, whether they are listed on any list of targeted financial sanctions, whether they have any connection to industries associated with higher ML/TF/PF risks, use an unverifiable source of funds, and whether they may use foreign companies to conduct the transaction.

It may be necessary to pay closer attention to customers that choose to use cash or make payments by or delivery through third parties as well as those that may appear to engage in structuring⁶.

3. **Business Counterparty Risk**- this includes the degree of ML/TF/PF risk posed by business counterparties. Higher risk counterparties include persons who⁷:
 - Proposes a transaction that makes no sense, or that is excessive, given the circumstances, in amount, or quality, or potential profit.
 - Makes frequent and unexplained changes in bank accounts, especially among banks in other countries.
 - Will not identify beneficial owners or controlling interests, where this would be commercially expected.
 - Seeks anonymity by conducting ordinary business through accountants, lawyers, or other intermediaries, see the paragraph above.

⁶ [FATF RBA GUIDANCE FOR DEALERS IN PRECIOUS METAL AND STONES](#), 17 June 2008

⁷ [FATF RBA GUIDANCE FOR DEALERS IN PRECIOUS METAL AND STONES](#), 17 June 2008

- Uses money services businesses or other non-bank financial institutions for no apparent legitimate business purpose.
 - Uses cash in its transactions with the dealer in precious metals or dealer in precious stones, or with his own counterparties in a nonstandard manner.
 - Is a politically exposed person (PEP) and/ or immediate family members, close personal or professional associate of a PEP.
4. **Transaction risk-** This type of risk considers the methods of financing used by customers and other parties to a transaction. In assessing this risk, you should take into consideration your regular business practices and encourage use of the regulated financial system to when conducting transactions. Cash transactions for high value transactions should be discouraged.

Circumstances which may indicate higher transaction risk includes, but are not limited to, the use of third parties, oversees accounts or persons/entities from higher risk jurisdictions to send or receive funds, the use of unusual means to finance the transaction, or unexplained and abrupt changes in financing arrangements.

5. **Product/service risk-** This risk is associated with the product you offer. For example, diamonds and pure gold are attractive as they represent a high value in a small package and they can be used as currency worldwide. By paying attention to and properly identifying your customers of gold and diamonds you can reduce the risk presented by anonymous, irregular transactions.⁸

Please see the FATF's Guidance "[RBA GUIDANCE FOR DEALERS IN PRECIOUS METAL AND STONES](#)" dated 17 June 2008, for more information on adopting a risk based approach and the risk factors relative to Dealers in Precious Metals and Stones to be considered.

Upon completion of your risk assessment, your [compliance programme](#) should be tailored to provide for the specific policies, procedures and controls to mitigate against the risks identified. These include documenting the appropriate Customer Due Diligence measures which ought to be applied for large transactions (TT\$50,000.00 or higher) and in higher and lower risk circumstances.

Please also visit our website for further guidance on [adopting a risk based approach](#).

⁸ [Implementing AML/CFT Measures in the Precious Minerals Sector: Preventing Crime While Increasing Revenue](#), prepared by Emmanuel Mathias and Bert Feys, International Monetary Fund, August 2014 and FATF's [RBA Guidance for Dealers in Precious Metals and Stones](#)

IV. DEVELOP AND IMPLEMENT A COMPLIANCE PROGRAMME

Regulation 7 of the FORs requires you to develop a written Compliance Programme (“CP”) to include specific policies, procedures and controls necessary for meeting the entity’s AML/CFT/CPF obligations.

The CP is a written document which should include the risk assessment that you have conducted for your particular business, as well as your system of internal policies, procedures, and controls which are intended to mitigate the vulnerabilities and inherent risks identified in your risk assessment, which can be exploited by money launderers and terrorism financiers.

After development of your CP, you must ensure that the CP is approved by senior management, effectively implemented and that the appropriate procedures are followed in a timely manner. Jewellers are also required to regularly review their AML/CFT/CPF measures and test them for effectiveness. As the AML/CFT/CPF Supervisory Authority, the FIUTT is empowered to examine the effectiveness of the implementation of the measures outlined in your Compliance Programme.

Please click here for the FIUTT’s guidance on [Compliance Programme](#).

V. CONDUCTING CUSTOMER DUE DILIGENCE

Your CP should contain policies and procedures for conducting Customer Due Diligence (“CDD”) in the appropriate circumstances. This includes setting out the specific procedures which must be followed when conducting transactions with higher and lower risk customers.

Jewellers should aim to ensure they conduct business solely with customers (including local and foreign suppliers) they can reasonably confirm are engaging in legitimate business. In meeting such obligation, Jewellers should implement adequate and reasonable measures to establish the identity of their customers and ensure the funds utilized to purchase any category of precious metals, stones and other jewellery are provided by the purchaser and not by a third party purchaser.

Part III of the FORs sets out the necessary approach to conducting CDD, which supervised entities must follow when entering into a business relationship with a customer or when conducting transactions with customers.

Additionally, the FIUTT has issued detailed guidance on measures, which should be taken when conducting CDD. This guidance can be found [here](#).

Please note that in addition to the general ML/TF/PF risk factors contained in the CDD guidance, risk factors specific to the business of Jewellery should be considered when risk rating clients for the purposes of CDD.

VI. TRAINING

Training is an essential component in combatting of money laundering, the financing of terrorism and financing of proliferation of weapons of mass destruction.

Regulation 6 of the FORS mandate that arrangements be made for training and ongoing training of the Directors and all members of staff to equip them to:

- (a) perform their AML/CFT/CPF obligations;
- (b) understand the techniques for identifying any suspicious transactions of suspicious activities; and
- (c) Understand the money laundering threats posed by new and developing technologies.

It is the responsibility of the Jeweller to develop on-going training programmes for the Compliance Officer, alternate Compliance Officer, owners/Directors and members of staff at the appropriate levels of the business.

Please [click here](#) to access the FIUTT's website for further information on training.

VII. INTERNAL AND EXTERNAL AUDIT

Regulation 10 of the FORs requires you to engage the services of internal and external auditors to review the CP for your business.

In reviewing the CP, the external auditor is required to evaluate your business' compliance with relevant AML/CFT/CPF legislation and guidelines; and submit reports generated and recommendations annually to the relevant Supervisory Authority. The internal auditor must ensure that your policies, procedures and systems comply with the FORs and that the level of transaction testing is in line with the risk profiles of your customers.

Please note that in the circumstances where you fail to engage the services of an external or internal auditor, the FIUTT will assign a competent professional, at your cost, to perform the relevant functions highlighted above.

Further guidance on engaging auditors to conduct the internal and external audits can be found [here](#).

VIII. SUBMISSION OF REPORTS TO THE FIUTT

As a supervised entity, you are required to submit three (3) types of reports to the FIUTT:

- **Suspicious Transactions Reports or Suspicious Activities Reports (STRs/SARs);**
- **Terrorist Funds Report (TFR); and**
- **Economic Sanctions Report (ESR)**

The relationship between reporting entities and the FIUTT is a key one given that the FIUTT can only perform its analytical function to produce financial intelligence if the various reporting entities report critical information they may have.

- Reporting Suspicious Transactions and Activities

You **MUST** submit a Suspicious Transaction Report or Suspicious Activity Report (STR/SAR) to the FIUTT where ***you know or have reasonable grounds to suspect that:***

- i. funds being used for the purpose of a transaction are the proceeds of a criminal conduct (*See S55A of the POCA*);
- ii. a transaction or an attempted transaction is related to the commission or attempted commission of a Money Laundering offence
- iii. an attempted transaction is related to a Terrorist Financing (*see Section 22C(2) of ATA*) or Proliferation offence (*see Clause 9 (2) of ESOs*); or
- iv. funds within the entity are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism (*See S22C (3) of the ATA*).

The STR/SAR must be submitted to the FIUTT within fourteen (14) days of the date the transaction was **deemed** to be suspicious (*See S55A (3) of the POCA and S 22C (6) of the ATA*)

- Reporting Terrorist Property/Funds

A Reporting Entity is required to screen its customers/clients against the following lists:

- (a) [United Nations Security Council Resolution \(UNSCR\) 1267/1989/2253 Sanctions List](#) and [United Nations 1988 Sanctions Committee List](#)

(together referred to as the “List of Designated Entities” in accordance with section 2(1) of the ATA⁹); and

- (b) [Trinidad and Tobago Consolidated List of Court Orders](#);

Screening of your clients should occur at the following two (2) stages:

- (a) At the on-boarding stage; **and**
- (b) *Immediately and without delay* upon receipt of a notification from the FIUTT that the List of Designated Entities and/or Consolidated List of High Court Orders has been updated.

If you identify that your client’s name appears on either of the above-mentioned lists, you are required to submit a TFR **immediately** to the FIUTT.

For Guidance on reporting Terrorist Property or Funds as it relates to the relevant form and procedure please click [here](#).

- Reporting Property/Funds for the Proliferation Financing of weapons of mass destruction.

You are required to immediately complete and submit an Economic Sanctions Report (“ESR”) to the FIUTT if upon screening your client against the List of Entities subject to a freezing High Court Order under the ESOs which is circulated by the Attorney General, you have acquired knowledge or reasonable suspicion that the client’s property/ funds is that of such listed entity. *(See Clause 9 of the ESOs)*

For Guidance on reporting Property or funds for Proliferation Financing as it relates to the relevant form and procedure please click [here](#).

⁹ Please note that both the ISIL (Da'esh) & Al-Qaida Sanctions Committee List - UNSCR 1267/1989/2253, and the UN Security Council Sanctions Committee Established Pursuant to Resolution 1988 (Taliban) List are contained in the [United Nations Security Council Consolidated List](#). If you have consulted the United Nations Security Council Consolidated List, you would have consulted both the ISIL (Da'esh) & Al-Qaida Sanctions Committee List - UNSCR 1267/1989/2253, and the UN Security Council Sanctions Committee Established Pursuant to Resolution 1988 (Taliban) Lists, together with all other lists maintained by the UN Security Council.

o *Defining Knowledge and Suspicion*

The first criterion above provides that, before you become obliged to report, you must **know** or **have reasonable grounds for suspecting**, that some other person is engaged in ML/TF/PF.

If you actually 'know' that your client is engaged in such a criminal activity, then your situation is quite straightforward – the first criterion is met.

Reasonable grounds to suspect

Having 'reasonable grounds to suspect' requires you to have more than mere suspicion, meaning that there is a possibility that a ML/TF/PF offence has occurred.

To have 'reasonable grounds to suspect', you are expected to have considered the facts, context and ML/TF/PF indicators related to a financial transaction and, having reviewed this information, you concluded that there are in fact reasonable grounds to suspect that the particular financial transaction is related to the commission of an ML/TF/PF offence. You need not verify the facts, context or ML/TF indicators that led to your suspicion.

You do not need to prove that an ML/TF/PF offence has actually occurred. Your suspicion however must be reasonable and not biased or prejudiced.

Attempted Transactions

If a client 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 FIUTT, and you must discontinue the business transaction or relationship with the entity.

An attempt is only when concrete action has been taken to proceed with the transaction.

Jewellers are reminded that once a STR/SAR is submitted to the FIUTT, all efforts must be employed to avoid any attempts at tipping off a person that an investigation is about to commence or has commenced or that a report was made to the FIUTT.

o *How to identify a Suspicious Transaction or Activity*

Determining whether a transaction or activity is suspicious is based on your knowledge of the customer and of the industry. You and your employees, if any, are better positioned to identify transactions which lack justification or do not fall within the usual methods of legitimate business. While there may be general indicators of suspicious transactions, there are also indicators specific to the business of dealing in precious metals and stones which would help you and your

employees to better identify suspicious transactions whether completed or attempted.

For examples of Suspicious Indicators as it relates to Jewellers, see the FIUTT's [Advisory to Jewellers and Financial Institutions: The Purchase of Jewellery/Gold Relative to Money Laundering](#)

For further guidance on Reporting STRs/SARs as it relates to procedure and associated offences, [click here](#).

IX. RECORD KEEPING

As a supervised entity you are required to retain records, including those related to transactions and client identification, for a period of six (6) years in electronic or written form. Retention of these records and the exercise of proper record keeping practices enable you to comply with lawful requests for information from auditors, other competent authorities and law enforcement authorities that request these records for the purposes of criminal investigations or prosecutions (*See Regulation 31 of the FORS*).

For further information on your record keeping obligations please see the FIUTT's [Guidance to Supervised Entities on Record Keeping](#).

5. GENERAL OFFENCE FOR FAILURE TO COMPLY WITH THE REGULATIONS AND FORS

Non-compliance with your obligations under the AML/CFT/CPF laws and regulations may result in criminal and or administrative sanctions.

Contravention of the POCA

A FI or LB which does not comply with Sections 55, 55A and 55C or any regulations made under Section 56 of the POCA, commits an offence and is liable on summary conviction, to a fine of five hundred thousand dollars and to imprisonment for a term of two years and on conviction on indictment, to a fine of three million dollars and to imprisonment for a term of seven years. (*See Section 57 of the POCA*)

Contravention of the FORS

A FI or LB which does not comply with the FORs, commits an offence and is liable on summary conviction, to a fine of five hundred thousand dollars and to imprisonment for a term of two years and on conviction on indictment, to a fine of three million dollars and to imprisonment for a term of seven years. *(See Section 57 of the POCA and Regulation 42 of the FORs)*

Contravention of the FIUTT Regulations

Where a FI or LB commits an offence under the FIUTT Regulations where no penalty is specified, it shall be liable on summary conviction, to a fine of twenty-five hundred thousand dollars and to a further fine of twenty-five thousand dollars for each day that the offence continues; and on conviction on indictment, to a fine of one million dollars and to a further fine of fifty thousand dollars for each day that the offence continues. *(See Regulations 36 and 37 of the FIUTT Regulations)*

Contravention of the ATA

A FI or LB which fails to comply with Section 22AB or Section 22C (1), (2) or (3) of the ATA commits an offence and is liable on summary conviction to a fine of five hundred thousand dollars and to imprisonment of two years and on conviction on indictment, a fine of three million dollars and imprisonment for seven years. *(See Section 42(1) of the ATA)*

Where a company commits an offence under Section 22AB or Section 22C (1), (2) or (3) of the ATA, any officer director or agent of the company who directed, authorized, assented to, or acquiesced in the commission of the offence or to whom any omission is attributable, is a party to the offence and is liable in summary conviction or conviction on indictment in the same manner as the above paragraph. *(See Section 42(2) of the ATA).*

Contravention of the ATA Regulations

A FI or LB which does not comply with the ATA Regulations commits an offence and is liable on summary conviction to a fine of five hundred thousand dollars and to imprisonment of two years. *(See Section 42(1) of the ATA and Regulation 7 of the ATA Regulations).*

[Intentionally left blank]

APPENDIX 1 - CASE STUDIES

Case Study 1: Sale of gold used as justification for movement of funds to another jurisdiction – Costa Rica¹⁰

A company operating in country A frequently sent representatives to country B offering services to buy gold, jewellery and precious stones / metals above local market prices. As a consequence of this activity, high quantities of funds were transferred from country A to country B with the reason given that the funds will be used to buy gold. The funds were then withdrawn from financial institutions in country B as either cash or cheques very soon after the funds transfer were made. Little was known about the movement of the merchandise purchased.

The same organisation organised a significant event held at a luxurious hotel in country B, advertising an intention to buy gold. However, few clients were present at the event. Monies (of unknown source) said to be surplus to the cost of holding the event were then sent back to country A or sent to other countries where the company did not operate, with the argument that they would be used for similar events.

Source: Costa Rica FIU

Case Study 2: Buying and selling gold anonymously¹¹

A wholesaler in precious metals (wholesaler A), held various bank accounts in Belgium. Analysis of these accounts showed that the wholesaler 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. Company/trader B supplied used gold to wholesaler A and is paid in cash. Company/trader B also pays its gold suppliers in cash.

In its financial records, company/trader B records the supplying companies as private individuals, without any form of identification. Company/trader B is suspected to be a cover for the owners' illegal activities, i.e. laundering proceeds of crime by exchanging money. Wholesaler A was known to the police to engage in money laundering. Its customers are apparently mainly shops selling gold in Antwerp, private individuals and intermediaries that were all recorded as "private individuals" in the 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, larger quantities of gold were split up so the price would never be more

¹⁰ FATF REPORT [Money laundering / terrorist financing risks and vulnerabilities associated with gold](#), July 2015

¹¹ FATF REPORT [Money laundering / terrorist financing risks and vulnerabilities associated with gold](#), July 2015

than EUR 15 000, the threshold for anti-money laundering / countering the financing of terrorism (AML/CFT) reporting of cash transactions. Apart from company/trader B, other suppliers of wholesaler A's were also known to the police. This led to suspicion that wholesaler A was being used to launder criminal proceeds. Providing anonymity and cash payments attract customers from a criminal environment.

Source: Belgium Financial Intelligence Unit (FIU)

-END OF DOCUMENT-