AML/CFT GUIDANCE FOR DEALERS IN PRECIOUS METALS AND STONES (JEWELLERS)

PURPOSE AND CONTENTS

The Financial Intelligence Unit of Trinidad and Tobago ("the FIU") provides the following summary of the obligations under the Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) regime of Trinidad and Tobago for dealers in precious metals and stones (Jewellers).

The purpose of this guidance is to provide industry specific guidance for Jewellers on their legal obligations for measures to deter and detect money laundering and financing of terrorism activities. Because AML/CFT obligations are contained in several laws, amendments and regulations, it is easier for Jewellers to access in one place the relevant provisions pertaining to their obligations. This guidance uses plain language to explain the most common situations under the specific laws and related regulations which impose 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.

The use of the word "must" indicates a legislative requirement, "should" indicates a best practice and the word "may" states an option for you to consider.

This guidance, which is divided into TEN (10) Parts, includes:

(1) Clarification on the business activities to which it applies.
(2) The role and function of the FIU in the AML/CFT regime.
(3) An explanation of money laundering and financing of terrorism.
(4) The main AML/CFT legal obligations and how these should be applied.
(5) How to identify suspicious transactions and "red flags" specific to Jewellers.
(6) Links to FIU Publications and Forms which provide additional detailed guidance:
    - Customer Due Diligence guide;
    - STR/SAR reporting Form and guidelines;
    - Terrorist Funds reporting Form and guidelines;
    - How to build an effective compliance programme; and

- Offences and penalties.

PART 1

DO THESE OBLIGATIONS APPLY TO YOU?

These obligations apply to you if you are licensed to carry on the business of a dealer in precious metals and stones under the Licensing of Dealers (Precious Metals and Stones) Act Chap 84:06.

These obligations apply to you if you are an individual or company, partnership or firm that buys, sells or receives precious metals or precious stones, in the course of your business activities. If you are an employee of such individual, company, partnership or firm, these obligations are the responsibility of your employer. If you are licensed under the Pawnbrokers Act Chap 84:05 and you receive precious metals and stones in pawn these obligations also apply to you.

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.

Here are a few **key concepts**:

(1) you need to be buying, selling, or receiving these items in the course of your business activities. Both the purchase and the sale of precious metals, precious stones, or jewellery are covered.

(2) the concept of personal adornment is key as regards jewellery e.g., earrings, rings, bracelets, necklaces. Items like Faberge eggs or a frame that is gold plated would not be considered jewellery.

(3) non-precious materials would not be considered and as well not industrial diamonds or industrial gems.

PART 2

LISTED BUSINESS

Anti-Money Laundering and Counter-Financing of Terrorism is everyone's responsibility. It is important to note that all Jewellers, in common with all citizens of Trinidad and Tobago, are subject to the Proceeds of Crime Act ("the POCA") and the Anti-Terrorism Act ("the ATA"). However, legal obligations are imposed on certain individuals and businesses which face a greater risk of coming across crime proceeds and terrorist property than others. Business sectors which have been identified as more vulnerable include Attorneys-at-Law and Accountants when performing certain specific functions, Real Estate agents, Dealers in precious metals and precious stones dealers(s) and Trust and Company service providers, etc. These business sectors are identified as "Listed Businesses" under the First Schedule to the Proceeds of Crime Act, Chap. 11:27.

If you carry on the business activities described in Part 1, you are a Listed Business; you have to comply with legal obligations under the AML/CFT laws of Trinidad and Tobago and the FIU as your Supervisory Authority monitors your compliance.

The AML/CFT laws of Trinidad and Tobago in which you will find your obligations are:

(1) Proceeds of Crime Act, Chap: 11:27("the POCA") - applies to all persons, but certain offences such as failure to report and the "tipping-off" offences only apply to persons who are engaged in activities in the regulated sector.

(2) Anti-Terrorism Act, Chap: 12:07("the ATA") - establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. The Anti-Terrorism Act applies to all persons but certain offences such as the failure to report and "tipping-off" offences only apply to persons who are engaged in activities in the regulated sector.

(3) Financial Intelligence Unit of Trinidad and Tobago Act, 2009, Act No.11 of 2009;

(4) Financial Obligations Regulations, 2010;

(5) Financial Intelligence Unit of Trinidad and Tobago Regulations, 2011; and

(6) Financial Obligations (Financing of Terrorism) Regulations, 2011.

PART 3

ABOUT THE FIU

The FIU is Trinidad and Tobago's Financial Intelligence Unit. The FIU was established under the FIU Act pursuant to Recommendation 26 of the 40+9 Recommendations of the Financial Action Task Force (the FATF). Recommendation 26 (now Recommendation 29 of the FATF's 40 Recommendations) mandates every country in the world to have a FIU to serve as the information related arm in efforts to combat money laundering, terrorism and related crimes. The FIU was created as an administrative type FIU, in that it does not have law enforcement or prosecutorial powers. Rather, it is a specialised intelligence agency which is legally responsible for producing financial intelligence for Law Enforcement Authorities (LEAs).

The FIU became operational in 2010 when it was established by virtue of the proclamation of the FIU Act. It is an autonomous department within the Ministry of Finance and the Economy.

The FIU works in very close partnership with Financial Institutions and Listed Businesses to ensure that those individuals and entities, comply with their obligations to report certain information to the FIU and supervises and monitors Listed Businesses for compliance with their AML/CFT obligations.

PART 4

WHAT THE FIU DOES

(1) Analyses & Produces Intelligence Reports

Essentially, the FIU is responsible for producing financial intelligence that is then disclosed to LEAs for investigation. To do this, the FIU receives and requests financial information from various reporting entities such as banks, credit unions and other financial institutions, accountants, attorneys-at-law, money services businesses, art dealers, motor vehicle sales, real estate, private members' clubs - a total of seventeen (17) different reporting sectors that must provide financial information to the FIU.

On receipt of the information, the FIU analyses it and looks for links between the financial information received, other relevant information from different sources, intelligence provided by LEAs, as well as other international partners. Once the analysis leads to the belief that the transaction is related to suspicions of money laundering or terrorist financing, the FIU sends an intelligence report to LEAs who will investigate the matter. The LEAs who investigate intelligence reports from the FIU are the Commissioner of Police, Comptroller of Customs and Excise, Chief Immigration Officer and Chairman of the Board of Inland Revenue.

The FIU receives many reports of suspicious transactions from reporting entities; but within those reports are legitimate transactions. The FIU's analysis is therefore, to ensure that only those transactions on which there are reasonable grounds to suspect are related to money laundering or terrorist financing are disclosed to LEAs. Only transactional information and information relating to the suspicion of money laundering and terrorist financing are contained in the Intelligence report. For example, the name and other information on the person who actually submitted the report would not be provided to LEAs.

(2) Supervises for AML/CFT Compliance

Another important function of the FIU is the responsibility of ensuring compliance with obligations under the POCA, the ATA and the Regulations made under those Acts. The FIU is the Supervisor for Listed Businesses and Non-Regulated Financial Institutions which have obligations under those Acts and Regulations and is responsible for making sure that they are meeting those obligations. Jewellers are a Listed Business which is supervised by the FIU.

Activities related to our compliance mandate would be educating and providing guidelines (such as this one), enhancing public awareness of money laundering and financing of terrorism to allow entities who have AML/CFT obligations to be aware and know exactly what they need to do in terms of meeting their obligations. The FIU also approves compliance programmes, conducts on-site inspections and takes action to ensure that the law is being respected by the entities it supervises.

PART 5

WHAT IS MONEY LAUNDERING?

Money Laundering is the process by which funds derived from criminal activity ("dirty money") are given the appearance of having been legitimately obtained, through a series of transactions in which the funds are 'cleaned'. Its purpose is to allow criminals to maintain control over those proceeds and, ultimately, provide a legitimate cover for the source of their income.

For money laundering to take place, first, there must have been the commission of a serious crime which resulted in benefits/gains (illegal funds) to the perpetrator. The perpetrator will then try to disguise the fact that the funds were generated from criminal activity through various processes and transactions which may also involve other individuals, businesses and companies. There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., cars or jewellery) to passing money through legitimate businesses and "shell" companies or as in the case of drug trafficking or other serious crimes. The proceeds usually take the form of cash which needs to enter the financial system by some means.

There are three (3) acknowledged methods in the money laundering process. However, the broader definition of money laundering offences in POCA includes even passive possession of criminal property as money laundering.

(1) Placement

Criminally derived funds are brought into the financial system. In the case of drug trafficking, and some other serious crimes, such as robbery, the proceeds usually take the form of cash which needs to enter the financial system. Examples of Placement are depositing cash into bank accounts or using cash to purchase assets. Techniques used include Structuring - breaking up a large deposit transaction into smaller cash deposits and Smurfing – using other persons to deposit cash.

(2) Layering

This takes place after the funds have entered into the financial system. It involves the movement of the money. Funds may be shuttled through a web of multiple accounts, companies and countries in order to disguise their origins. The intention is to conceal, hide, and obscure the money trail in order to deceive the law enforcement and to make the paper trail very difficult to follow.

(3) Integration

The money comes back to criminals as apparently legitimate funds. The laundered funds are used for activities such as investment into real estate, luxury assets, and business ventures, to fund further criminal activity or spent to enhance the criminal's lifestyle. At this stage, the illegal money has achieved the appearance of legitimacy.

Successful money laundering allows criminals to use and enjoy the income from the criminal activity without suspicion.

PART 6

WHAT IS FINANCING OF TERRORISM?

Financing of Terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity. Funds may involve low dollar value transactions and give the appearance of innocence and a variety of sources. Funds may come from personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organise fundraising activities where the contributors to the fundraising activities believe that the funds will go to relief efforts abroad, but, all the funds are actually transferred to a terrorist group. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism you may have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place.

However, like money launderers, terrorism financiers also move funds to disguise their source, destination and purpose for which the funds are to be used. The reason is to prevent leaving a trail of incriminating evidence - to distance the funds from the crime or the source, and to obscure the intended destination and purpose.

PART 7

WHY ARE JEWELLERS A LISTED BUSINESS?

The 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.

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. Terrorist groups have engaged in the gemstone trade for a long time. Historically, they engaged extensively in the profit-making trade in diamond, tanzanite, amethyst, ruby and sapphire. However, according to recent intelligence, gemstones, diamonds in particular, are being 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.

FATF has acknowledged the vulnerability of dealers in precious metals and precious stones by recommending that such business activity should be subject to AML/CFT requirements. All countries in the world have to have laws which put these requirements on Jewellers.

Examples of ML cases involving Jewellers.

Case 1 - Diamonds are a Launderer's Best Friend

A lawyer of Country Y absconded with millions of US dollars from his "customer escrow" account. Investigations revealed that part of these funds was used to purchase loose diamonds and jewellery from a local jeweller in Country Y.

This case illustrates the use of direct purchase of precious stones to launder the crime proceeds. In particular, it shows the way for an absconder to conceal and move the proceeds of crime across different countries.

Case 2 - Limited Edition Jewellery

Expensive Jewellery Limited (EJL), a foreign firm active in a small jurisdiction, noted that it was attracting an increasing number of very affluent customers.

The owners of EJL considered that, in the same way there was a market in the jurisdiction for prestige, limited edition cars, there was also a market for very expensive, limited edition jewellery and forged business links with foreign firms to market high value jewellery.

Occasionally, selected customers were invited to the jurisdiction to attend viewings. Sometime after it developed this new business line, EJL auctioned a diamond necklace. The necklace was sold for a sum in excess of £1 million to a buyer who was represented at the auction by his agent.

Payment was made to the auctioneer's bank account as agreed. The bank informed the auctioneer that the £1million had been received but payment had been made from different companies via three different banks in different jurisdictions.

This information led the auctioneer to think that all was not quite right with this purchase and he made a disclosure to the local financial investigation unit. It was discovered through intelligence that the agent and his customer had drug trafficking convictions and were suspected of several frauds and laundering the proceeds of their own and other frauds.

PART 8

YOUR OBLIGATIONS

As a Jeweller, your main obligations under the AML/CFT laws are summarized below:

(1) *Register with the FIU;*

(2) *Submit Reports to the FIU ;*

(3) *No "Tipping-off";*

(4) *Keep Records;*

(5) *Ascertain customer identity;*

(6) *Ascertain whether the customer is acting for a Third Party;*

(7) *Appoint a Compliance Officer;*

(8) *Develop an effective Compliance Programme and submit to the FIU; and*

(9) *Implement your Compliance Programme and conduct periodic reviews.*

(1) REGISTRATION WITH THE FIU

You must register with the FIU for the purpose of identifying yourself as an entity which is supervised by the FIU if you perform any of the specified activities. You must also notify the FIU of a change of address of your registered office or principal place of business.

Businesses in existence on or before February 10, 2011 were required to register within three (3) months from the coming into effect of the FIU Regulations, i.e. by May 9, 2011.

If you commenced business after May 9, 2011 you must register as soon as you begin operations or as soon as you register under the Registration of Business Names Act or incorporate or register under the Companies Act, whichever is the earlier date.

a) How to Register

The registration process is very simple and free of charge. On-line registration is available through the FIU's website or you may download the form and complete it manually. You may register on the FIU Registration Form which you may access by **clicking here**.

b) Offences

Failure to register within the time stipulated is an offence and 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.

Failure to notify the FIU of a change of address of your registered office or principal place of business is an offence and you are liable on summary conviction to a fine of $20, 000.

(2) SUBMITTING REPORTS TO THE FIU

You are required to send to the FIU two (2) types of reports

a) reports of Suspicious Transactions or Activities; and

b) reports of Terrorist Funds in your possession.

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

Failing to report to the FIU knowledge or suspicion of crime proceeds or terrorist property is a criminal offence. If you continue to deal with such a transaction or funds knowing or having reasonable grounds to believe that the funds are crime proceeds or terrorists' funds and you do not report it to the FIU then you may have committed the offence of money laundering or financing of terrorism.

a) Reporting Suspicious Transactions/Activities

i. You **must submit a suspicious transaction or activity report (**STR/SAR) to the FIU where you know or have reasonable grounds to suspect:

- ❖ that funds being used for the purpose of a transaction are the proceeds of a crime; or
- ❖ a transaction or an attempted transaction is related to the commission or attempted commission of a money laundering offence; or

- ❖ that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organizations or those who finance terrorism.

The STR/SAR must be submitted within fourteen (14) days of the date the transaction was deemed to be suspicious.

ii. You **must submit a STR/SAR to the FIU 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 Security Council of the United Nations. **You may access the Security Council of the United Nations List ("the UN list") by clicking here.**

iii. 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 FT.

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 by a jury 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 realise that the activity concerned amounted to money laundering.

iv. 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 FIU.

Example of suspicious attempted transaction: a customer wants to purchase a $10,000 necklace, and to pay in cash, and you, as a Jeweller, 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 FIU. 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 is the underlying criminal activity or whether illegal activities occurred.

You must report suspicious transactions/activities and terrorist funds **on the STR/SAR Form which you may access by clicking here.**

Click here for **Guidance Note on Suspicious Transaction/Activity Reporting Standards to guide you in completing the STR/SAR form.**

v. 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 atypical 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.

In making your assessment, consider the following red flags when you buy, sell or receive in pawn Precious Metals and Stones:

- 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, traveller'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 other than TT dollars.
- 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 pawns 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 may be suspicious. Money laundering includes the layering and integrating stages where there is no more cash, but only funds that are moved around while trying to confuse the

money trail. It can also be of any amount. If you think a $ 1,000.00 transaction is suspicious, you must report it to the FIU.

b) Reporting Terrorist Funds

i. You **must report immediately** to the FIU 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.

ii. You **must report immediately** to the FIU where you know or have reasonable grounds to believe that a person or entity named on the UN list or the list circulated by the FIU, has funds in Trinidad and Tobago.

Report the existence or suspicion of terrorist funds on the **Terrorist Funds Report - FIU TFR Form** which you may access by **clicking here**.

You may access the **Security Council of the United Nations List ("the UN list")** by **clicking here**.

Click here for **Guidance Note on Procedures for Reporting Terrorist Funds** to assist you in completing the TFR form.

(3) NO TIPPING-OFF

When you have made a suspicious transaction report to the FIU, you or any member of your staff must not disclose that you have made such a report or the content of such report to any person including the Customer. 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 your behalf, including any agent, employee, partner, director or other officer, or any person engaged under a contract for services.

(4) RECORD KEEPING

You 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.

You must keep the following records in electronic or written form for a period of six (6) years or such longer period as the FIU directs. The records must be kept for six (6) years after the end of the business relationship or completion of a one-off transaction.

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 Compliance Officer (STRs/SARs);
g) A register of copies of suspicious transaction reports submitted to the FIU (STRs/SARs);
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 transfers records; (originator and recipient identification data) and
k) Other relevant records.

(5) ASCERTAIN CUSTOMER IDENTITY – KNOW YOUR CUSTOMER

If you cannot satisfactorily apply your due diligence measures in relation to a Customer, e.g, you are unable to identify and verify a Customer's identity or obtain sufficient information about the nature and purpose of a transaction, you must **NOT** carry out a transaction for that Customer or enter into a business relationship with the Customer and you must terminate any business relationship already established. You should also consider submitting a STR/SAR to the FIU.

a) **All Customers**

You must **identify** who is the prospective customer and **verify** the person's identity by reference to independent and reliable source materials. Such material should include documentary identification issued by the Government departments or agencies. You must also ask the source of funds for the transaction. Customer's identification, also called CDD or Know Your Customer–KYC, must be obtained for customers who are individuals as well as companies. You must obtain satisfactory evidence of the Customer's identity before establishing a business relationship or completing a transaction for occasional *customers.*

Click here for **Customer Due Diligence Guide No. 1 of 2011** for more information.

b) High Risk Customers/Transactions

There are customers and types of transactions and products which may pose higher risk to your business and you are required to take additional measures in those cases. The AML/CFT laws have identified certain high risks 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 take specific measures to identify and verify the identity of the following individuals or entities:

i. Any individual or entity who conducts a large cash transaction i.e. TT $90,000 and over;
ii. Any individual or entity who conducts business transactions with persons and financial institutions in or from other countries which do not or which insufficiently

comply with the recommendations of the Financial Action Task Force ("the FATF"). Click here for **FATF High Risk and Non-Cooperative Jurisdictions**;

iii. Any individual or entity who conducts a complex or unusual transaction, (whether completed or not), unusual patterns of transactions and insignificant but periodic transactions which have no apparent economic or visible lawful purpose;.

iv. Domestic and Foreign Politically Exposed Persons (PEPs). Click here **for Customer Due Diligence Guide No. 1 of 2011** for the categories of persons who are PEPs;

v. Any individual or entity for whom you have to send a suspicious transaction report to the FIU (reasonable measures and exceptions apply e.g., to avoid tipping-off);

vi. Any customer or transaction, product type that you have identified as posing a higher risk to your business; eg pawn-broking transactions, cash transactions over $10,000.00.

EDD measures to apply to high risk customers include but is not limited to:

- Verification of identity using independent sources e.g., additional form of Government issued identification;
- Obtaining details of the source of the customer's funds and the purpose of the transaction;
- Obtaining approval from the senior officer to conduct the transaction;
- Applying supplementary measures to verify or certify the documents supplied or requiring certification by a financial institution;
- Imposing a cash threshold limit for transactions after which a senior officer's approval is needed to conduct the transaction;
- Verifying the source of funds for the transaction e.g., if Customer states the money is from his bank account, ask for proof.
- Ongoing monitoring (e.g., monthly, quarterly or on a transaction basis) of the Customer's account through the relationship; or
- Obtaining details about the source of items in pawn-broking transactions.

(6) Is the Customer acting for a Third Party?

You must take reasonable measures to determine whether the Customer is acting on behalf of a third party especially where you have to conduct EDD.

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 has 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.

Click here for **Customer Due Diligence Guide No. 1 of 2011** for more information.

(7) APPOINT A COMPLIANCE OFFICER

You must appoint a senior employee at managerial level as Compliance Officer (CO). The individual you appoint will be responsible for the implementation of your compliance regime.

You must obtain the approval of the FIU for the person you have chosen as your CO. If you change your CO you must inform the FIU immediately and get the FIU's approval for the new CO.

If you are a small business, employing five (5) persons or less, the CO must be the person in the most senior position. If you are the owner or operator of the business and do not employ anyone, you can appoint yourself as CO to implement a compliance regime.

In the case of a large business (employing over five [5] persons), the CO should be from senior management and have direct access to senior management and the board of directors.

Further, as a good governance practice, the appointed CO in a large business should not be directly involved in the receipt, transfer or payment of funds.

Your CO should have the authority and the resources necessary to discharge his or her responsibilities effectively. The CO must:

a) have full responsibility for overseeing, developing, updating and enforcing the AML/CFT Programme;
b) have sufficient authority to oversee, develop, update and enforce AML/CFT policies and procedures throughout the company; and
c) be competent and knowledgeable regarding money laundering issues and risks and the anti-money laundering legal framework.

Depending on your type of business, your CO should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator of the business. The identity of the CO must be treated with the strictest confidence by you and your staff.

The CO's responsibilities include:

i. Submitting STRs/SARs and TFRs to the FIU and keeping relevant records;
ii. Acting as Liaison officer between your business and the FIU;
iii. Implementing your Compliance Programme;
iv. Directing and enforcing your Compliance Programme;
v. Ensuring the training of employees on the AML/CFT; and
vi. Ensuring independent audits of your Compliance Programme.

For consistency and on-going attention to the compliance regime, your appointed CO may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the CO retains full responsibility for the implementation of the compliance regime.

Best practice: You should appoint an alternate CO to perform the CO's functions in the event the CO is absent for any reason. You will need to obtain the FIU's approval for the person to act as alternate CO.

(8) DEVELOP AND SUBMIT TO THE FIU A WRITTEN COMPLIANCE PROGRAMME

After you have registered with the FIU as a reporting entity, you must develop a written Compliance Programme ("CP"). If you are an organization, the CP also has to be approved by senior management. You must submit the CP to the FIU and you should submit the CP checklist as well to assist the FIU in its review of the CP.

The CP is a written document explaining your system of internal procedures, systems and controls which are intended to make your business less vulnerable to being used by money launderers and terrorism financiers. Your CP will contain measures that ensure that you comply with your reporting, record keeping, customer identification, employee training, and other AML/CFT obligations. These policies, procedures and controls, must be communicated to employees, and when fully implemented, will help reduce the risk of your business being used for money laundering or to finance terrorism. The CP must be reviewed every two (2) years.

The FIU will examine your CP and approve or recommend amendments if deficiencies are identified.

A well-designed, applied and monitored regime will provide a solid foundation for compliance with the AML/CFT laws. As not all individuals and entities operate under the same circumstances, your compliance procedures will have to be tailored to fit your individual needs. It should reflect the nature, size and complexity of your operations as well as the vulnerability of your business to money laundering and terrorism financing activities.

The following five (5) elements must be included in your compliance regime:

a) The appointment of a staff member as CO;

b) Internal compliance policies and procedures;

c) Your assessment of your risks to money laundering and terrorism financing, and measures to mitigate high risks;

d) Ongoing compliance training for staff; and

e) Periodic documented review of the effectiveness of implementation of your policies and procedures, training and risk assessment.

Click here to access the **Guide to Structuring an AML/CFT Compliance Programme and** click here **for the CP checklist.**

(9) IMPLEMENT AND TEST YOUR COMPLIANCE PROGRAMME

Your obligations include implementing your written CP. The FIU may conduct an onsite examination to determine whether the measures outlined in your CP are effectively implemented.

In addition, you must conduct internal testing to evaluate compliance by you and your staff with your CP in particular, CDD, record keeping and suspicious transactions reporting. Best practice indicates that internal testing should be carried by someone other than the CO, to avoid potential conflict since the CO is responsible for implementation of the CP, its measures and controls.

External testing must also be carried out to test the effectiveness of your systems, controls and implementation of same by someone not employed in your business.

If you are the CO as well as the most senior employee (person at the highest level in the organization) an external independent review, will comply with your obligation to test your implementation of your AML/CFT obligations.

Such reviews (both internal and external) must be documented and made available to the FIU.

PART 9

OFFENCES & PENALTIES FOR NON-COMPLIANCE

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

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

Click here to access a summary of the Offences and Penalties under AML/CFT laws and regulations of Trinidad and Tobago.

PART 10

ADDITIONAL RESOURCES

This summary is intended to guide you in fulfilling your legal obligations under the AML/CFT Laws.

Additional reference materials include:

- The AML/CFT laws available on the FIU's website, www.fiu.gov.tt under **"Legal Framework".**
- FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Stones - updated Feb 1, 2012 at http://www.fatf-gafi.org/documents/riskbasedapproach/fatfguidanceontherisk-basedapproachfordealersinpreciousmetalsandstones.html
- The FATF recommendations at www.fatf-gafi.org/recommendations

Published on May 23, 2013

****