AML/CFT GUIDANCE FOR THE TRUST AND COMPANY SERVICE PROVIDERS

PURPOSE AND CONTENTS

The Financial Intelligence Unit of Trinidad and Tobago ("the FIU") provides the following overview of the obligations under the Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) regime of Trinidad and Tobago for Trust and Company Service Providers (TCSPs).

The purpose of this guidance is to provide compliance guidance for TCSPs on their legal obligations to deter and detect Money Laundering and Financing of Terrorism activities. Because AML/CFT obligations are contained in several laws, amendments and regulations, our aim is that TCSPs will find this guidance useful to access the relevant provisions pertaining to their obligations in one place. 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 AML/CFT Acts and Regulations.

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

This guidance, is divided into ten (10) parts and includes:

1.	Do these obligations apply to you? – Clarification on the specified business activities which apply to TCSPs.
2.	What is a Listed Business?
3.	The role and function of the FIU in the AML/CFT regime.
4.	What is Money Laundering?
5.	What is Financing of Terrorism?
6.	Why are Trust and Company Service Providers a Listed Business?
7.	Examples of Money Laundering using TCSPs.

8.	What are your AML/CFT legal Obligations? - An explanation of the main AML/CFT legal obligations, how they should be applied and Best Practices.
9.	Offences & Penalties.
10.	Additional Resources.
	Appendix – Suspicious Transactions/Activities Indicators

PART I

DO THESE OBLIGATIONS APPLY TO YOU?

Clarification on the specified business activities which apply to the TCSPs

Trust and Company Service Providers have the meaning used by the Financial Action Task Force (FATF) and thus includes all those persons and entities that, on a professional basis, participate in the creation, administration and management of trusts and corporate vehicles.

These obligations apply to you if you are a TCSP which operates within Trinidad and Tobago and which prepares for and carries out the specified transactions described below.

If you are an employee of a company, sole practitioner or firm or partnership, these requirements are the responsibility of your employer but you as an employee will have internal reporting of suspicious transactions and terrorist property obligations in accordance with your employer's compliance programme.

If you are a company, sole practitioner, firm or partnership, you are subject to the obligations explained in this guideline if you perform the following specified activities on behalf of any individual or entity (other than your employer).

As such, these obligations apply to you as a TCSP if by way of business, you provide services or prepare for and carry out transactions for a third party in relation to the following activities:

a) acting as a formation agent of legal persons;
b) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons;
c) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
d) acting as (or arranging for another person to act as) a nominee shareholder for another person; or
e) acting as (or arranging for another person to act as) a trustee of an express trust.

Some terms explained:

Acting as (or arranging for another person to act as)

Arranging for someone to act in a particular capacity has a specific meaning here. An example would be if you provided a client with a company director, selecting them without further reference back to your client and completing some or all of the formalities to appoint them.

It does not include the normal process of headhunting or advertising to find a suitable candidate for a position that a recruitment agency would carry out.

Directors, Shadow Directors and Nominee Directors/Shareholders

You count as director of a company if:

- you are formally appointed as a director and your name is registered at the Companies
- Registry;
- you are a 'shadow director' - you direct or control the business but you are not formally appointed as a director;
- you are a nominee director if you have been appointed by a third party instead of the shareholders in general meeting. This manner of their appointment distinguishes nominee directors from the ordinary director.

A nominee shareholder holds shares on behalf of the actual owner (the beneficial owner) under a contractual agreement. The shares will be recorded in the name of the nominee.

If you are simply called a director as part of your job title without being formally appointed you may not fall within this remit.

PART 2

WHAT IS A LISTED BUSINESS?

Anti-Money Laundering and Counter-Financing of Terrorism is everyone's responsibility. It is important to note that all TCSPs, 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, further obligations are imposed on business sectors 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 TCSPs. A T C S P i s o n e o f t h e business sectors 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. Your obligations apply to those activities identified where there is a high risk of Money Laundering or Financing of Terrorism occurring.

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")** as amended by Act No. 15 of 2014 - applies to all persons, but certain offences such as failure to report suspicious transactions only apply to Listed Business and Financial Institutions.

(2) **Anti-Terrorism Act, Chap. 12:07 ("the ATA")** as amended by Act No 15 of 2014 - establishes several offences for engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. The ATA applies to all persons but certain offences such as the failure to report suspicious transactions only apply to Listed Business and Financial Institutions.

(3) **Financial Intelligence Unit of Trinidad and Tobago Act, 2009, Chap. 72:01 ("the FIU Act")**as amended by Act No. 15 of 2014;

(4) **Financial Obligations Regulations 2010**; as amended by The Financial Obligations (Amendment) Regulations, 2014 (LN No.392);

(5) **Financial Intelligence Unit of Trinidad and Tobago Regulations 2011** as amended by the Financial Intelligence Unit of Trinidad and Tobago (Amendment) Regulations, 2014 (LN No. 403); and

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

These laws are available on the FIU's website http://www.fiu.gov.tt/

PART 3

THE ROLE AND FUNCTION OF THE FIU IN THE AML/CFT REGIME

The FIU is Trinidad and Tobago's Financial Intelligence Unit. The FIU was established under the FIU Act pursuant to Recommendation 29 of the 40 Recommendations of the Financial Action Task Force (the FATF). Recommendation 29 mandates all its member jurisdictions to have a FIU to serve as the information related arm in efforts to combat Money Laundering, Financing of 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 upon the proclamation of the FIUTT Act. It is an autonomous department within the Ministry of Finance.

The FIU works in very close partnership with individuals and entities that have obligations under the AML/CFT laws. Those entities within the art sector have such obligations and are therefore also reporting entities.

WHAT THE FIU DOES

(1) Analyses and Produces Intelligence Reports

Essentially, the FIU is responsible for **producing financial intelligence** that is then disclosed to law enforcement agencies (LEAs) for investigation. To do this, the FIU receives suspicious transaction or suspicious activities reports (STRs/SARs) 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 **must** make (STRs/SARs) to the FIU.

The FIU receives many reports of suspicious transactions/activities 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 to ensure compliance with obligations under the POCA, the ATA, the FIU Act 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.

Activities related to the FIU's compliance mandate include educating and providing guidelines (such as this one), and 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 with regard to meeting their obligations. The FIU also conducts on-site inspections and takes action to ensure that the law is being complied with by the entities it supervises.

PART 4

WHAT IS MONEY LAUNDERING?

The offence of money laundering is the process by which illegally obtained funds are given the appearance of having been legitimately obtained. Money laundering begins with the commission of criminal activity 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., art, 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.

(1) Placement

'Placement' refers to the process by which funds derived from criminal activity are introduced 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 property/assets. Techniques used include Structuring or 'smurfing'- where instead of making a large deposit transaction and in order to avoid suspicion or detection the illegal receipts are broken up into smaller sums and deposited into single or multiple accounts sometime using other persons are used to deposit the cash.

(2) Layering

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

(3) Integration

The money comes back to criminals "cleaned", as apparently legitimate funds. The laundered funds are used to fund further criminal activity or spent to enhance the criminal's lifestyle. Criminals may use your services to assist in investment in legitimate businesses or other forms of investment, to buy a property, set up a trust, acquire a company, or even settle litigation, among other activities.

Successful Money Laundering allows criminals to use and enjoy the income from the criminal activity without suspicion.

PART 5

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 may come from a variety of sources. Funds may come from personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organize 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 also originate from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike Money Laundering, with Financing of Terrorism you may have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place and may involve both legitimate funds as well as funds derived from criminal activity being used in support of executed and planned terrorist activity. 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 thereby avoiding suspicion or detection.

PART 6

WHY ARE TRUST AND COMPANY SERVICE PROVIDERS A LISTED BUSINESS?

The FATF, an inter-governmental body which sets international policies for Anti-Money Laundering and counter-Financing of Terrorism has found that Trust and Company Service Providers (TCSPs) play a key role in the global economy as financial intermediaries, providing an important link between financial institutions and many of their customers. They often provide invaluable assistance to clients in the management of their financial affairs and can therefore significantly impact transactional flows through the financial system. Further, TCSPs are often involved in some way in the establishment and administration of most legal persons and arrangements and accordingly in many jurisdictions they play a key role as the gatekeepers for the financial sector.

Lawyers, accountants, notaries and other such professionals provide services to clients to help them navigate the often complex and sometimes treacherous world of finance, law and corporate governance. They have essential knowledge and expertise in relation to the technical rules and regulations that pertain to the operation of business, as well as experience in crafting legal strategies in relation to investment, mergers and acquisitions, tax liability, corporate structuring, among others.

These professionals can be important service providers for businesses, high net worth investors and anyone who has wealth or assets which need to be managed or channelled appropriately. However, these same skills and expertise are attributes that are desired by criminals, who require assistance in organizing their affairs, to enable them to distance proceeds from their criminal origins and to liberate these proceeds for eventual use in 'legitimate' endeavours.

For this purpose criminals seek out the services of professional intermediaries to help them establish corporate structures, set up trusts, transfer funds and negotiate deals. The important advantages to the criminal are:

(1) The concealment of the proceeds of crime;

(2) The granting of access to various financial centres through the diverse mechanisms which can be used by these intermediaries;

(3) The creation of confusing audit trails to stymie law enforcement's efforts with regard to these transactions.

Whilst the majority of TCSPs appear to be established for legitimate purposes, it is clear from the research that some TCSPs are being used, unwittingly or otherwise, to help facilitate the above and thus includes all those persons and entities that, on a professional basis, participate in the creation, administration and management of trusts and corporate vehicles.

FATF'S Recommendation 22 requires countries to ensure that this class of business is subject to effective systems for monitoring and is compliant with AML/CFT measures.

NCIAL INTELLIGENCE

PART 7

EXAMPLES OF MONEY LAUNDERING CASES INVOLVING TCSPS*

Case No. 1: Vulnerability arising from lack of AML/CFT oversight

This case occurred in 2002, when one of the directors of a trust company business operating in Country X was approached to set up a discretionary trust by a solicitor in Country Y. The solicitor advised that one of his clients, Mr. A, was acting on behalf of another individual, Mr. B. Mr. A had received monies from the sale of sauna business, which was owned by Mr. B. The solicitor wished to hold the sale proceeds through an offshore trust. The solicitor sent through documents to identify Mr. A, but none in relation to the ultimate client Mr. B. A few days later, over $850,000 was sent from the solicitor's account to the trust company's client account. Two days later, the solicitor requested the trust company to pay the bulk of those monies to four named entities, none of which had any connection to the trust and which were unknown to the trust company. The trust was established with Mr. A as the sole beneficiary. On the next working day, the trust company made the four payments as requested.

The High Court of Country X found both the trust company and the director of the trust company guilty of failing to comply with client identification requirements of the anti-money laundering law, a decision which was upheld by the Court of Appeal. The Court of Appeal found that an isolated failure to comply with client identification procedures in the context of financial services business can amount to a criminal offence and that a systemic failure is not required. It was held that Client identification procedures prescribed by the anti-money laundering law must be kept up and that a single breach, provided that it was more than a mere oversight, is sufficient to constitute an offence.

Submitted by JE

Case No. 2: Criminal culpability of TCSPs as facilitator of ML

A Company Formation Agent involved in the financial services sector was prosecuted for money laundering offences, for laundering funds on behalf of organized crime groups. He carried out a complex process of funnelling criminal proceeds through a system of trusts and front and shell companies, linked to a complex matrix of inter-account bank transfers. As administrator of all the trusts used in the scheme he exercised full control of the funds flowing through them. Trusts, as well as front and shell companies were used deliberately to disguise the source of the money, and to provide a veil of legitimacy to the financial transactions.

Source: submitted by the GB

AL INTELLIGE

Case No. 3: Use of professional intermediaries to facilitate money laundering

A criminal involved in smuggling into Jurisdiction A set up a Trust in order to launder the proceeds of his crime, with the assistance of a collusive Independent Financial Adviser (IFA) and a Solicitor, who also appeared to be acting in the knowledge that the individual was a criminal. The Trust was discretionary and therefore power over the management of the fund was vested in the Trustees, namely the criminal, his wife and the IFA.

This example illustrates the complexity of Trusts used to hide the origins of funds from any law enforcement scrutiny. One way in which this was done was through the purchase of a garage. The criminal's daughter, who was a beneficiary, was given the property by her father and she in turn leased it to a company. The property was eventually sold to this company, the purchase funded by a loan provided by the Trust. The company subsequently made repayments of several thousand pounds a month, ostensibly to the Trust, but in practice to the criminal. Thus the criminal who had originally owned the garage probably maintained control despite his daughter's ownership. Through controlling the Trust he was able to funnel funds back to himself through loaning funds from the Trust and receive payments on that loan.

Source: submitted by GB

*Cases *taken from FATF Report October 2010 – Money Laundering using Trust and Company Service Providers.*

PART 8

WHAT ARE YOUR AML/CFT LEGAL OBLIGATIONS?

The AML/CFT laws of Trinidad and Tobago impose obligations on you to:

i. Register with the FIU;
ii. Submit Reports to the FIU;
iii. Not to "Tip-off";
iv. Keep Records;
v. Ascertain client identity;
vi. Ascertain whether the client is acting for a Third Party;
vii. Appoint a Compliance Officer and Alternate Compliance Officer;
viii. Develop a written effective Compliance Programme; and
ix. 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 within six (6) months of such change.

You must register with the FIU within three (months) of commencing business activity or incorporation as a company, whichever is the earlier date.

You must also notify the FIU where there is a change of Directors, Owners, Partners or Compliance Officer within six (6) months of such change.

I. *How to Register*

The registration process is very simple and free of charge. On-line pre-registration is available through the FIU's website however you must download the form and print the completed registration form. To complete the registration process you must sign your printed pre-registration form and **manually submit this to the FIU**.

Register on **the FIU Registration Form** which you may access by **clicking here.**

II. *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.
- Failure to notify the FIU of a change of Directors, Owners, Partners or Compliance Officer within six (6) months will be an offence and you will be 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:

(1) reports of Suspicious Transactions or Activities (STRs/SARs) ; and

(2) 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.

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) Reports of Suspicious Transactions/Activities

i. You must submit a Suspicious Transaction Report or Suspicious 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 also** submit a STR/SAR to the FIU **immediately** if a terrorist 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 such entity.

***A terrorist entity means any individual or entity and their associates designated as terrorist entities by the Security Council of the United Nations or any individual or entity listed under section 22B ATA appearing on the consolidated list of High Court Orders as maintained and circulated by the FIU.**

Report using the **STR/SAR 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 **STR Reporting Standard No 1 of 2011** to guide you in completing the STR/SAR form.

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 Financing of Terrorism.

If you actually 'know' that your client 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, for example, 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 client 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 or Financing of Terrorism. The main purpose of the objective test is to ensure that TCSPs (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, e.g. 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 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 FIU.

Example of suspicious attempted transaction: a visitor walks into your art gallery. He says he would like to buy a painting for his living room; he has $ 10,000 in cash to spend. He says his name is John X but when you ask him for identification he replies that he left it in his car. You insist he provide it. He goes away to get it but does not return. If you think from all the information you have that this is unusual or the transaction is related to some crime you have to report that attempted transaction to the FIU.

NOTES:

It is only when *you know or have reasonable grounds to suspect* that the funds are criminal proceeds or related to Money Laundering or Financing of Terrorism that you have to report: you do not have to know what the underlying criminal activity is or whether illegal activities have actually occurred.

Money Laundering can take place with any amount of money/cash. If you think a $ 1,000 transaction is suspicious, you must report it to the FIU.

You must report suspicious transactions/activities and attempts by a terrorist entity* to enter into a transaction or continue a business relationship **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. Identifying a Suspicious Transaction/Activity

TCSPs should pay particular attention to the Money Laundering risks presented by the services which they offer to avoid being manipulated by criminals seeking to launder illicit proceeds. TCSPs are encouraged to make reasonable enquiries if they come across information which could form the beginning of a suspicion.

You are the one to determine whether a transaction or activity is suspicious based on your knowledge of the client 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, whether the transaction is normal for that particular client or is it a transaction which is atypical i.e. unusual as well as the payment methods.

What are the risk indicators for the Trust and Company Service Provider Sector?

In making your assessment, consider some of the functions performed by TCSPs that are the most useful to the potential launderer such as:

- Financial and tax advice – Criminals with large sums of money to invest may pose as individuals hoping to minimize their tax liabilities or desiring to place assets out of reach in order to secure future liabilities;
- Creation of corporate vehicles or other complex legal arrangements (e.g. trusts) - such structures may serve to confuse or disguise the links between the proceeds of a crime and the criminal and obscure the beneficial owners and controllers of the company;
- Buying or selling of property – Property transfers serve as either the cover for transfers of illegal funds (layering stage) or else they represent the final investment of these proceeds after the proceeds have passed through the laundering process (integration stage);
- Performing financial transactions – TCSPs may carry out various financial operations on behalf of the client (e.g. cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing cheques, purchase and sale of stock, sending and receiving international funds transfers etc.); and
- Gaining introductions to financial institutions.

The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious, will depend on various factors such as the type of client and the transaction or service in question. Industry- specific indicators would also help you and your employees to better identify suspicious transactions whether completed or attempted.

Consider the following red flags when you act on behalf of a client:

- Activities which have no apparent purpose, or which make no obvious economic sense (including where a person makes an unusual loss), or which involve apparently unnecessary complexity;
- The use of non-resident accounts, companies or structures in circumstances where the
- client's needs do not appear to support such economic requirements;
- Where the activities being undertaken by the client, or the size or pattern of transactions are, without reasonable explanation, out of the ordinary range of services normally requested or are inconsistent with your experience in relation to the particular client:
    - Lack of transparency in beneficial ownership information
    - Excessively obstructive or secretive client
    - Client is reluctant to provide identity documents
    - Purpose of instructions, legal services and transactions is unclear
    - Transactions involve unusual levels of funds or cash
    - Property transactions which are atypical
    - Transactions involving countries on the FATF's list of NCCTs
    - Transactions related to offshore business activity
    - Changing instructions

It is important to note that it is not only cash transactions which may be suspicious. Money Laundering includes the layering and integration 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 transaction is suspicious, you must report it to the FIU.

The **Appendix** attached provides further details on these suspicious transaction indicators.

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**.
You may also access the FIU's Consolidated List of High Court Orders ("the Consolidated 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 the fact or content of such report to any person. It is an offence to inform any person, including the customer, that you have or your business has filed a suspicious transaction report about the customer's transactions.

You must also not disclose to anyone any matter which may prejudice a Money Laundering or Financing of Terrorism investigation or proposed investigation.

(4) RECORD KEEPING

You are required to keep a record of each and every transaction for a specified period. Record keeping is important for use in any investigation into, or analysis of, possible Money Laundering or Financing of Terrorism offences. Records must be kept in a manner 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 format *for at least 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:

- ✓ All domestic and international transaction records
- ✓ Source of funds declarations
- ✓ Client identification records
- ✓ Client information records
- ✓ Copies of official corporate records
- ✓ Copies of suspicious transaction reports submitted by your staff to your Compliance Officer
- ✓ A register of copies of suspicious transaction reports submitted to the FIU
- ✓ A register of all enquiries made by any Law Enforcement Authority or other competent authority
- ✓ The names, addresses, position titles and other official information pertaining to your staff
- ✓ All Wire transfers records (originator and recipient identification data)
- ✓ Other relevant records.

(5) ASCERTAINING IDENTITY – KNOW YOUR CLIENT

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

a) All Clients

The general principle is that a TCSP should establish satisfactorily that they are dealing with a real person or organization (not fictitious) and obtain identification evidence sufficient to establish that the client is who they say there are or a legitimate organization. In the case of an organization, you must ascertain that the client is duly authorized to act for the organization.

You must **identify** who is the prospective client and **verify** the person's identity by reference to independent and reliable source material. Such material should include documentary identification issued by the Government departments or agencies. You must also ask the source of funds for the transaction where enhanced due diligence (EDD) would be necessary. Client's identification, also called Customer Due Diligence (CDD) or Know Your Client (KYC) must be obtained for clients who are individuals as well as companies. You must obtain satisfactory evidence of the client's identity before establishing a business relationship or completing a transaction for occasional clients.

***Best Practices*:**

1. While TCSPs are not obliged by the AML/CFT laws to identify, or perform any of the other CDD measures on clients when the services provided to them fall outside of the AML/CFT specified activities, the FIU recommends that TCSPs should identify all clients to whom they wish to provide any legal service and verify their identification documents as a sound risk management measure. Therefore, TCSPs should apply the AML/CFT standards when arranging the establishment of, or providing services in relation to, any legal entities not covered in Part 1 above (e.g. a foundation).

2. Those individuals holding key positions in the TCSP such as a director or senior manager/officers should be persons of integrity and should have no relevant adverse business/professional/personal history.

3. TCSP should ensure that there is proper provision for holding, having access to and sharing of information, including ensuring that –

   i) information on the ultimate beneficial owner and/or controllers of companies, partnerships and other legal entities, and the trustees, settlor, protector/beneficiaries of trusts is known and is properly recorded;

   ii) any change of client control/ownership is promptly monitored (e.g. in particular when administering a corporate vehicle in the form of a "shelf" company or nominee share holdings are involved).

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

b) High Risk Clients/Transactions

There are circumstances where the risk of money laundering or terrorist financing is higher and Enhanced Due Diligence (EDD) measures have to be taken. You must take specific measures to identify and verify the identity of the following high risk persons (individuals or entities):

i. Any individual or entity who conducts a large cash transaction i.e. over TT $90,000;

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"); and

vi. Any client or transaction or service or product type that you have identified as posing a higher risk to your business e.g., transactions which involve high levels of funds or cash.

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

i. Obtaining additional information on the customer e.g., additional form of Government issued identification;

ii. Obtaining details of the source of the client's funds and the purpose of the transaction if relevant;

iii. Verifying the source of funds for the transaction e.g., if client states the cash is from his bank account, ask for proof;

iv. Obtaining approval from a senior officer to conduct the transaction;

v. Applying supplementary measures to verify or certify the documents supplied or requiring certification by a financial institution;

vi. Ongoing monitoring (e.g., monthly, quarterly, annually or on a transaction basis) of the client's account throughout the relationship; and

vii. Implementing any other customer identification policies and procedures to prevent money laundering and financing of terrorism.

***Best Practice*:**

Large payments made in actual cash may also be a sign of money laundering. A policy of not accepting cash payments above a certain limit or at all may reduce that risk. Since clients may attempt to circumvent such a policy by depositing cash directly into your client's account at a bank, you should avoid disclosing client's account details as far as possible and make it clear that electronic transfer of funds is expected.

c) Is the Client acting for a Third Party?

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

Such cases will include where the client 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 client.

In deciding who the beneficial owner is in relation to a client who is not a private individual, (e.g., a company or trust) you should look behind the corporate entity to identify those natural person(s) who have ultimate control over the business and the company's assets, with particular attention paid to any shareholders or others who inject a significant proportion of the capital or financial support.

Particular care should be taken to verify the legal existence and trading or economic purpose of corporates and 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.

VI. Is the Client acting for a Third Party?

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

Such cases will include where the client is an agent of the third party who is the beneficiary and who is providing the funds for the transaction.

In practice, this means that if the TCSP knows, or has reasonable suspicion to believe that the other party to a transaction is, in fact, acting on behalf of someone else they must establish the identity of the true beneficial owner and their relationship with the client. This identification of the beneficial owner should take place even if the identity is to ultimately remain unknown to third parties.

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

(6) 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 chosen as the CO. If you change your CO you must inform the FIU immediately and get the FIU's approval for the new CO.

You must also appoint an alternate for the CO ("ACO") who shall be a senior employee or such other competent professional as approved in writing by the FIU. The alternate shall discharge the functions of the CO in his absence.

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

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 CO 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.

(7) DEVELOP AND IMPLEMENT A 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 organisation the CP also has to be approved by senior management. **Click here for the CP Check list**.

The CP is a written document which includes a risk assessment of your particular business and which sets out your system of internal procedures, systems and controls which are intended to mitigate the vulnerabilities and inherent risks identified by you which can be exploited by money launderers and terrorism financiers. Your CP will contain measures that ensure that you comply with your reporting, record keeping, client 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.

It is advisable to revise the CP on a regular basis say every 2 years, to ensure that measures in place remain commensurate with the risks posed to the business and are current with legal obligations.

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:

(1) the appointment of a staff member as CO and his/her responsibilities;

(2) internal compliance policies and procedures such as reporting suspicious transactions to the CO; application of CDD, EDD and record keeping;

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

(4) ongoing compliance training for all staff at the level appropriate for their job duties; and

(5) periodic documented review/audits 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**

(8) IMPLEMENT AND TEST YOUR COMPLIANCE PROGRAMME

Your obligations include implementing your written CP. The FIU may conduct an onsite examination to determine the effectiveness of implementation of the measures outlined in your CP.

All employees involved in the day-to-day business of a TCSP should be made aware of the policies and procedures in place in the business to prevent Money Laundering and Financing of Terrorism.

You must conduct internal testing to evaluate compliance by your staff with your CP, in particular, CDD record keeping and suspicious transactions reporting.

In addition, you must conduct internal testing and external independent testing to evaluate the effectiveness of your systems and controls and implementation of same. Such reviews must be documented.

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 the AML/CFT laws and regulations of Trinidad and Tobago**.

This summary is intended to guide you in fulfilling your legal obligations under the AML/CFT laws. You may access the laws on the FIU's website, www.fiu.gov.tt under **"Legal Framework".**

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". Click here** to access the laws.
- FATF Report – Money Laundering using Trust and Company Service Providers – October 2010 - at http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingusingtrustandcompanyserviceproviders.html
- The FATF recommendations at www.fatf-gafi.org/recommendations

Published on February 24, 2014

Updated September 18, 2017

Susan S. François
Director of the Financial Intelligence Unit

APPENDIX

AML/CFT SUSPICIOUS TRANSACTIONS/ACTIVITIES – INDICATORS

- Transactions that require the use of complex and opaque legal entities and arrangements;
- The payment of "consultancy fees" to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies;
- The transfer of funds in the form of "loans" to individuals from trusts and non-bank shell companies. These non-traditional "loans" then facilitate a system of regular transfers to these corporate vehicles from the "borrowing" individuals in the form of "loan repayments";
- Cases of corruption where the company paying the bribe to secure a contract or the person brokering a contract will seek to secure a successful outcome by utilising a TCSP to operate a trust with the funds held on deposit for the benefit of the person approving the contract;
- The use of TCSPs in jurisdictions that do not require TCSPs to capture, retain or submit to competent authorities information on the beneficial ownership of corporate structures formed by them;
- The use of legal persons and legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs;
- The use of legal persons or legal arrangements that operate in jurisdictions with secrecy laws;
- The use by prospective clients of nominee agreements to hide from the TCSP the beneficial ownership of client companies;
- The carrying out of multiple intercompany loan transactions and/or multijurisdictional wire transfers that have no apparent legal or commercial purpose;
- Clients who require the use of pre-constituted shell companies in jurisdictions that allow their use but do not require updating of ownership information; and
- TCSPs that market themselves and/or their jurisdictions as facilitating anonymity and disguised asset ownership.

Please note that this is not an exhaustive list of suspicious indicators.