AML/CFT GUIDANCE FOR 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 industry specific 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, it would be easier for the TCSPs 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 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) 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 Obligations? - The main AML/CFT legal obligations and how these should be applied.

(9) Offences & Penalties

(10) Additional Resources

Appendix – Suspicious Transactions/Activities Indicators

**PART 1**

**DO THESE OBLIGATIONS APPLY TO YOU?**

Trust and Company Service Providers’ has 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 TCSP is one of the 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”)** - applies to all persons, but certain offences such as failure to report and the “tipping-off” 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 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 and “tipping-off” only apply to persons who are engaged in activities in the regulated sector.
FIU Confidential

(3) Financial Intelligence Unit of Trinidad and Tobago Act, 2009, Chap. 72:01 (“the FIU Act”);
(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.
(1) Analyses and 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 the 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.
Activities related to our compliance mandate would be educating and providing guidelines (such as this one), enhancing public awareness of Money Laundering and terrorist financing 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 4

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’. Money Laundering allows 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.
(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 and involves the movement of the funds. 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 and to make the paper trail very difficult to follow.

(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 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 6**

**WHY ARE TRUST AND COMPANY SERVICE PROVIDERS A LISTED BUSINESS?**

The FATF, a 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: the concealment of the proceeds of crime; the granting of access to various financial centres through the diverse mechanisms which can be used by these intermediaries; and 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 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 24 requires countries to ensure that this class of business is subject to effective systems for monitoring and is compliant with AML/CFT measures.
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 money 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 organised 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

**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 OBLIGATIONS?

As a TCSP, 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 client identity;
6. Appoint a Compliance Officer;
7. Appoint a Compliance Officer;
8. Develop and submit to the FIU a written Compliance Programme; and
9. Implement and test 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.

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.

**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.

TCSPs should consider whether they should continue to act for a client when they have to submit a STR/SAR on that client. A relevant factor to consider would be whether they reasonably believe that to
delay or to stop or the failure to proceed might make a client suspicious that a report may be or may have been made or that an investigation may commence or already has commenced.

a) Reporting 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 that 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 Suspcion
      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.

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 client wants you to form a company for him. He is vague on what are the proposed company’s business activities and he presents you with $10,000 in cash to cover your fees and incorporation fees. You ask him for identification and he delays in providing it but keeps pressing you to form the company; subsequently he terminates the transaction. If you think that this transaction is related to some crime you have to report the attempted transaction to the FIU. On the other hand, a client simply seeking your advice on how to form a company and how long it takes would not be sufficient for being an attempted transaction.

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

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; is the transaction normal for that particular client or is it a transaction which is atypical i.e. unusual; as well as the payment methods.

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.

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

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 client. It is an offence to deliberately tell any person, including the client, that you have or your business has filed a suspicious transaction report about the client’s activities/transactions. You must also not
disclose to anyone any matter which may prejudice Money Laundering or Financing of Terrorism investigation or proposed investigation.

The prohibition applies to any person acting, or purporting to act, on behalf of a Trust and Company Service Provider or firm, 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 for use in any investigation into, or analysis of, possible Money Laundering or terrorist financing. 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 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) Client’s identification records;

d) Client’s information records;

e) Copies of official corporate records;

f) Copies of Suspicious Transaction Reports (STRs/SARs) submitted by your staff to your Compliance Officer;

g) A register of copies of Suspicious Transaction Reports (STRs/SARs) submitted to the FIU;

h) A register of all enquiries (date, nature of enquiry, name of officer, agency and powers being exercised) made by any LEA 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’s identification data); and

k) Other relevant records.
(5) **ASCERTAIN CLIENT 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 he is dealing with a real person or organization (not fictitious) and obtain identification evidence sufficient to establish that the client is that person or 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. 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 clients and types of transactions, services and products which may pose higher risk to your business and you are required to apply additional measures in those cases. The AML/CFT laws have identified certain high risks clients and require you to conduct Enhanced Due Diligence (“EDD”) on
these clients. You may also determine that certain clients, 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 high risk 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 clients, which include, but are not limited to:

- Verification of identity using independent sources e.g., additional form of Government issued identification;

- Obtaining details of the source of the client’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;

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

- Ongoing monitoring (e.g., monthly, quarterly, annually or on a transaction basis) of the client’s account throughout the relationship.
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 who has 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.
(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.

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 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.

**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.

(7) 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.

Click here for the CP Check list.

The FIU will examine your CP and approve or recommend amendments if deficiencies are identified.
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 terrorist 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. The CP must be reviewed every two (2) years.

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.

<table>
<thead>
<tr>
<th>The following five (5) elements must be included in your compliance regime:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) The appointment of a staff member as CO and his/her responsibilities;</td>
</tr>
<tr>
<td>b) internal compliance policies and procedures such as reporting suspicious transactions to the CO; application of CDD, EDD and record keeping;</td>
</tr>
<tr>
<td>c) your assessment of your risks to money laundering and terrorism financing, and measures to mitigate high risks;</td>
</tr>
<tr>
<td>d) ongoing compliance training for all staff at the level appropriate for their job duties; and</td>
</tr>
<tr>
<td>e) periodic documented review of the effectiveness of implementation of your policies and procedures, training and risk assessment.</td>
</tr>
</tbody>
</table>

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 whether the measures outlined in your CP are effectively implemented.

All employees involved in the day-to-day business of a TCSP should be made aware of the policies and procedures in place in their firm to prevent money laundering and Financing of Terrorism risks. You must conduct internal testing to evaluate compliance by your staff with your CP, in particular, CDD record keeping and suspicious transactions reporting. Best practice indicates that internal testing should be carried out by someone other than the CO, to avoid potential conflict since the CO is responsible for implementation of the CP, its measures and controls.

PART 9

OFFENCES AND 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”.

The FATF recommendations at www.fatf-gafi.org/recommendations

APPENDIX

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.

Published on February 24, 2014