Version no: 2.1
Date Prepared: 30/09/2017
Last Date Revised: 25/02/2026

GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO

Ministry of Finance

AML/CFT/CPF GUIDANCE FOR TRUST AND COMPANY SERVICE PROVIDERS

Purpose

This Guidance is intended to provide assistance to TCSPs registered with the FIUTT with their AML/CFT/CPF obligations.

FIUTT REFERENCE: GN/006/2025
Version 2.1 updated 25 February 2026

VERSION	DATE	AUTHOR	DESCRIPTION	APPROVED BY	STATUS
1.0	30/09/2017	Legal Division	Approved Final Version	Director FIUTT	Final
2.0	25/11/2025	Legal Division	Approved Final Version	Director FIUTT	Final
2.1	10/02/2026	Legal Division	Updated to reflect amendments made to the FIUTTRs via Act No. 7 of 2025. The hyperlinks were updated throughout the document.	Director Legal Services	Final

Table of Contents

1. INTRODUCTION

A Trust and Company Service Provider ("TCSP") is a Listed Business *(also referred to a "supervised entity")* described in the First Schedule of the POCA as any such person when he prepares for and when he carries out transactions for a client 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; and
(e) acting as, or arranging for another person to act as a trustee of an express trust.

This Guidance is intended to provide assistance to TCSPs who are engaged in these activities on behalf of their clients, in complying with their Anti-Money Laundering, Counter Financing of Terrorism and Counter Proliferation Financing ("AML/CFT/CPF") legal obligations:

In accordance with the Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01 and the Proceeds of Crime Act, Chap. 11:27, the Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT") is the Supervisory Authority over all Listed Businesses, including TCSPs performing the afore-mentioned activities on behalf of a client.

Every TCSP conducting these activities is required to honour his/its AML/CFT/CPF obligations set out in the following Acts and Regulations:

1. The Financial Intelligence Unit of Trinidad and Tobago Act, Chapter 72:01 ("FIUTTA")
2. The Financial Intelligence Unit of Trinidad and Tobago regulations, 2011 ("FIUTT Regulations")
3. The Proceeds of Crime Act, Chapter 11:27 ("POCA")
4. The Financial Obligations Regulations, 2010 ("FORs")
5. The Anti-Terrorism Act, Chapter 12:07 ("ATA")
6. The Financial Obligations (Financing of Terrorism) Regulations, 2011 ("FO(FT)Rs")
7. The Counter-Proliferation Financing Act (Act No. 8 of 2025) ("CPFA")
8. The Counter-Proliferation Financing Regulations, 2025 ("CPFRs")
9. Economic Sanctions (Implementation of United Nations Resolutions on the Democratic People's Republic of Korea) Order, 2018 ("DPRK Order")
10. Economic Sanctions (Implementation of United Nations Resolutions on the Islamic Republic of Iran) Order, 2018 ("Iran Order")

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

into force of the CPFA, the FATF Compliance Act 2024 and the FATF Compliance Act 2025 and replaces all previous guidance issued specific to the TCSP Sector.

The Financial Action Task Force ("FATF"), which sets international policies for Anti-Money Laundering and Counter-Financing of Terrorism has found that TCSPs play a key role in the global economy as financial intermediaries, providing an important link between financial institutions ("FI") and many of their customers. Consequently, TCSPs often provide invaluable assistance to clients in the management of their financial affairs and can significantly impact transactional flows through the financial system. Further, TCSPs are often involved in the establishment and administration of most legal persons and arrangements and in many jurisdictions, play a key role as a gatekeeper for the financial economy. As such, TCSPs can be important service providers for businesses, high net worth investors and anyone who has wealth or assets which need to be managed or channeled appropriately.

However, in the same vein, the FATF acknowledges that 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' endeavors. For this purpose, criminals seek out the services of professional intermediaries such as TCSPs to help them establish corporate structures, set up trusts, transfer funds and negotiate deals. The important advantages to the criminal are as follows:

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

Consequently, while the majority of TCSPs are established for legitimate purposes, TCSPs may be used, unwittingly or otherwise, to help facilitate the above. The vulnerabilities of TCSP services are often seen in the formation of companies and trusts as well as predicate offences such as tax crimes that may be facilitated through the formation on legal entities.

Formation of companies and trusts

Criminals often see companies and trusts as instruments which can be used to retain control over the proceeds of crime while creating additional layers of ownership to frustrate the attempts of law enforcement to trace the ownership and origin of said proceeds. Shell Companies are a particular conduit for such misuse. Note that a shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.

Criminals may also seek to misuse shelf companies formed by TCSPs by seeking access to companies that have been 'sitting on the shelf' for a long time. A shelf company is an incorporated company with an inactive secretary, shareholders, and directors and has been left dormant for a long period, even if a customer relationship has already been established. Shelf companies may be used in an attempt to create a false impression that the company has been in existence and operation for an extended time. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

The risks presented herein are not exhaustive and TCSPs are encouraged to conduct further research to determine whether their particular services are at risk for misuse by criminals for ML, its predicate offences, TF or PF.

(Source - FATF (2019), Risk-based Approach for Trust and Company Service Providers , FATF, Paris FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers (fatf-gafi.org)*,)*

WHY SUPERVISE TCSPs?

The requirement, for TCSPS carrying out the specified activities, to register with the FIUTT and comply with AML/CFT/CPF obligations enables them to effectively mitigate these risks and ultimately avoid such potential misuse.

For additional scenarios demonstrating the misuse of TCSPs for money laundering, please see Appendix 1

2. DO THESE OBLIGATIONS APPLY TO YOU?

These obligations apply to you if you are an individual or company, firm or partnership who performs the specified activities listed in the First Schedule of the POCA and further explained below. If you are an employee of such individual, company, firm or partnership these obligations are the responsibility of your employer but you as an employee will have obligations to report suspicious transactions to the Compliance Officer of your organisation in accordance with your employer's compliance programme.

Specified Activities:

a) **Acting as a formation agent of legal persons.** This specified activity refers to services provided by you in the formation and incorporation of a Legal Person or Legal Arrangement. This includes assisting with the preparation of and/or filing of incorporation and post incorporation documents with the Companies Registry on behalf of a client.

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.** This activity applies to you if you provide services to a client whereby you act as a director of a company or provide corporate secretarial services to a company, whether incorporated, unincorporated, for profit or not for profit, or act as a partner of a partnership on behalf of a client. This also includes situations where you find other persons to act in the above positions, and/or prepare documentation for another person to act in the above positions.

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.** This activity refers to providing a physical address whereby mail, other correspondence and items intended for the Legal Person or Legal Arrangement will be received on behalf of the Legal Person or Arrangement, whether to be forwarded to the intended recipient or picked up.

d) **Acting as (or arranging for another person to act as) a nominee shareholder for another person** This activity applies to you if you provide this service for your clients who are legal persons or if you find persons and prepare or file the necessary documentation for another person to perform this service for your clients

e) **Acting as, or arranging for another person to act as a trustee of an express trust.** If you are acting in this capacity, you provide a service to clients where you agree to be the Trustee of an express trust, or if you find persons and prepare or file the necessary documentation for another person to perform this Trustee service for your clients.

NB - *A Trust is a legal instrument where a person (the trustee) controls funds or property for the benefit of another person (the beneficiary). An Express Trust is one which is created knowingly and intentionally (usually by way of a document).*
E.g. a revocable living trust – this can give a trustee the power to make decisions about another person's funds or property while that person is still alive; a charitable trust – which donors can donate funds or property for the management of the trustee on behalf of other beneficiaries; or a trust created upon death through a Will to provide property to a minor whereby such property will be managed by another person until the minor becomes of age.

[Intentionally left blank]

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

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

I. Registration with the FIUTT
II. Appoint a Compliance Officer and Alternate Compliance Officer
III. Assessing AML/CFT/CPF Risks
IV. Develop and implement a Compliance Programme
V. Conducting Customer Due Diligence
VI. Internal and External Audits
VII. Submission of Reports to the FIUTT
VIII. Keep Records

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

I. REGISTRATION WITH THE FIUTT

You **must** register with the FIUTT if you are performing any of the specified activities of a TCSP for or on behalf of other individuals or entities. Your application for registration must be received within thirty (30) days from the date of incorporation as a company or commencing business activity, whichever is the earlier. *(See Section 18B of the FIUTTA and Regulation 28(1) of the FIUTT Regulations).*

Please note that once you obtain a Certificate of Registration, that Certificate will be valid for a period of five (5) years from the date of the Certificate. Subsequently, you will be required to renew your registration with the FIUTT if you wish to continue conducting Supervised Activities as explained in section 3.

To register with the FIUTT, , and learn more about the renewal of registration process, you may visit the FIUTT's website to access the **FIUTT Registration of Supervised Entities Forms** and **relevant instructions**.

Please note that pursuant to Regulation 28(2) of the FIUTT Regulations, failure to register with the FIUTT within the time stipulated is an offence for which you are liable on summary conviction to a fine of $50,000 and to a further fine of $5,000 for each day the offence continues. You may also be subject to an administrative fine of $25,000.00 and a further fine of $1000.00 per day for each day you continue to fail to submit your application for registration with the FIUTT.

- Changes in particulars and to senior management or beneficial owners

You are required to notify the FIUTT where there is a change of your registered office or principal place of business; your business name, company name or trading name; or the nature of your business. You are also required to notify the FIUTT of a change to your Directors, Beneficial Owners, Legal Owners, Partners or Compliance Officer.

Notification of these changes must be made in writing, within thirty (30) days of the change.

Submissions of such changes can be made manually or electronically.

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

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

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

You may also be subject to an administrative fine of $10,000.00 and a further fine of $500.00 per day for each day you continue to fail to notify the FIUTT of the aforementioned changes.

- De-registration

In the circumstances where your entity is no longer performing the business activities of a TCSP as described above, it is advised that an application for de-registration be made to the FIUTT *(See Section 18BA of the FIUTTA)*. In order to deregister with the FIUTT, you must first ensure that your business is **not** engaged in **any** business activity listed on the FIUTT's **List of Supervised Sectors**.

To deregister with the FIUTT, you must submit:

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

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

In the case of a Registered Business, you are required to submit copy of your Notice of Cessation (Form 9), as the legal presumption is that the business is being carried on, as long as the business name remains on the Register of Business Names[1].

Submissions for deregistration can be made manually or electronically.

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

Once the FIUTT is satisfied that you are no longer performing the activities which requires you to be registered, your application for deregistration will be accepted and you will be issued with a Notice of De-registration. In addition, your entity's name will be removed from the FIUTT's List of Registrants, inserted to the FIUTT's List of De-Registrants, and uploaded on our website. A notice will also be circulated to the Financial Institutions informing them of same. It should be noted that de- registration from the FIUTT will not affect any other form of business activity but only financial transactions pertaining the specified activities which require FIUTT registration.

The FIUTT may also deregister your entity if it becomes aware that it, its legal or beneficial owners, directors or senior officers is a listed entity under the ATA or the ESOs; or are found to no-longer be fit and proper under sections 18BB(2) or (3) of the FIUTTA.

If the FIUTT becomes so aware, it will serve your entity with a Notice of Intention to Deregister and give your entity an opportunity to make written representations to the FIUTT if you are not in agreement with the reasons for deregistration.

II. APPOINT A COMPLIANCE OFFICER AND ALTERNATE COMPLIANCE OFFICER

Regulation 3(5) of the FORs requires you to designate a Compliance Officer for the purpose of securing compliance with AML/CFT/CPF obligations.

Regulation 3(8) of the FORs requires you to also appoint an alternate compliance officer who will be required to undertake the functions of the Compliance Officer should the Compliance Officer be absent from duty whether it be a short or extended period of time.

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

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

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

Compliance Officer, respectively. Please note that failure of an entity to train the Compliance Officer to enable them to perform their functions in accordance with Regulation 4(1) of the FORS is a very serious contravention and the entity may be subject to an administrative fine or summary conviction. (Please see the schedule at Regulation 42 of the FORS)

For guidance on designating a Compliance Officer and Alternate Compliance Officer, and receiving approval from the FIUTT, please click here.

III. ASSESSING RISK

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

Section 9 of the CPFA requires an entity to develop and implement policies and programmes which are reasonably designed on a risk sensitive basis to manage and mitigate proliferation financing risks to ensure compliance.

FATF advises in its Guidance for a Risk Based Approach for Trust And Company Service Providers (TSCPs), dated June 2019[2], that *"identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow TCSPs to determine and implement reasonable and proportionate measures and controls to mitigate such risks."*

This risk assessment should be documented and should include current and emerging ML/TF/PF trends while considering how such issues may impact the business.

Your risk assessment ought to follow an approach that considers, amongst other things, your particular client base, the size of your business, the financial value of transactions involving your business and the nature of such transactions. Note, however, that circumstances can vary widely depending on the nature of your role and involvement in the services you provide to each client.

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

1. **Geographical factors**- this includes noting the country/jurisdiction where your clients, parties to the transactions and/or the property involved, are from. You must consider the effectiveness of that country's AML/CFT/CPF regime, identified deficiencies and whether the country is subject to sanctions by international organisations. This can be done through conducting checks on the FATF's list of High Risk and other monitored jurisdictions and

[2] FATF (2019), Risk-based Approach for Trust and Company Service Providers (TSCPs), FATF, Paris, FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers (fatf-gafi.org).

jurisdictions under increased monitoring. The FIUTT regularly publishes FATF public statements of jurisdictions who have been added to and removed from these lists **here.**

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

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

   Higher risk circumstances for clients include, but are not limited to, whether the firm's client base includes sectors which are vulnerable to ML/TF/PF; the firm's clients include PEPs and their associates who are considered to be higher risk; or for clients which are companies and other legal persons – where there is unusual complexity in the control or ownership structure.

3. **Transaction risk/Service risk**- This type of risk considers the services provided by TCSPS which may be misused by criminals. Circumstances which may indicate higher transaction risk includes, but are not limited to, the use of pooled client accounts or safe custody of client money or assets without justification; situations where advice is sought on setting up legal arrangements in a manner which may be misused to obscure ownership or real economic purpose; or the use of virtual assets and other anonymous means of payment and wealth transfer without apparent legitimate reason.

Please see the FIUTT's Guidance to Supervised Entities on a Risk Based Approach to AML/CFT/CPF and Guidance to a Risk Based Approach to Counter Proliferation Financing for Reporting Entities for comprehensive guidance on conducting your Risk Assessment and implementing a Risk Based Approach.

You can also consider the FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers (fatf-gafi.org) for *more information on developing a risk based approach; and* ***Appendix II*** *for a list of red flags and suspicious indicators of which you should be cognizant.*

Upon completion of your risk assessment, your compliance program should be tailored to provide for the specific policies, procedures and controls to mitigate against the risks identified. These include documenting the appropriate Customer Due Diligence measures which ought to be applied for large transactions (TT$50,000.00 or higher) and in higher and lower risk circumstances. Entities are required to make available its documented risk assessment to the Supervisory Authority upon request in accordance with Regulation 7(2)(c) of the FORs.

Please also visit our website for further guidance on **adopting a risk based approach**.

IV. DEVELOP AND IMPLEMENT A COMPLIANCE PROGRAMME

Regulation 7 of the FORs and section 9 of the CPFA requires you to develop a written Compliance Programme ("CP") to include specific policies, procedures and controls necessary for meeting the entity's AML/CFT/CPF obligations.

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

The Compliance Programme must be approved by the senior management of the entity.

After development of your CP, you are required to ensure that it is effectively implemented and that the appropriate procedures are followed in a timely manner. As the AML/CFT/CPF Supervisory Authority, the FIUTT is empowered to examine the effectiveness of the implementation of the measures outlined in your Compliance Program.

Please click here for the FIUTT's guidance on **Compliance Programme**.

V. CONDUCTING CUSTOMER DUE DILIGENCE

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

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

The FIUTT has issued detailed guidance on measures which should be taken when conducting CDD. This guidance can be found **here**.

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

VI. TRAINING

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

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

(a) perform their AML/CFT/CPF obligations;

(b) understand the techniques for identifying any suspicious transactions or suspicious activities; and

(c) Understand the money laundering threats posed by new and developing technologies.

Regulation 6 of CPFA Regulations mandates that arrangements must be made for the training of directors in relation to counter-proliferation financing. Regulation 6(2) states that a programme of training shall include:

(a) procedures and controls for the prevention of the misuse of technological developments in the breach, evasion and non-implementation of targeted financial sanctions in relation to proliferation financing;

(b) new developments in methods and trends in the breach, evasion and non-implementation of targeted financial sanctions in relation to proliferation financing; and

(c) the appropriate internal controls and communication for the purpose of preventing the breach, evasion and non-implementation of targeted financial sanctions in relation to proliferation financing.

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

Please visit the FIUTT's website at AML/CFT Training – Financial Intelligence Unit for further information on training.

VII. INDEPENDENT REVIEWS

Regulation 10 of the FORs requires you to conduct an independent review of your compliance with the AML/CFT/CPF legislation and FIUTT's Guidance, and the reliability, integrity and completeness of the design and effectiveness of your compliance risk management function and your internal controls framework. This review is required to be conducted on a risk basis, at a minimum of every 3 years, or at such intervals as the FIUTT may require.

This independent review replaces the previous External and Internal Audit requirement by merging the functions of both the external and internal auditors for listed businesses. The Independent Review must be undertaken by a qualified professional who is sufficiently independent from all your entity's business lines. This independence allows for an unbiased review of all systems. It is

recommended that a suitably qualified AML/CFT/CPF audit professional be retained to fulfill this function.

In conducting the Independent Review the independent professional is required to evaluate your business' compliance with relevant AML/CFT/CPF legislation and guidelines; and submit reports and recommendations generated to the FIUTT at least every 3 years or at the frequency required by the FIUTT. The Independent professional must ensure that your policies, procedures and systems are functioning in keeping with the AML/CFT/CPF laws and the risk profiles of your customers.

VIII. SUBMISSION OF REPORTS TO THE FIUTT

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

- **Suspicious Transactions Reports or Suspicious Activities Reports (STRs/SARs);**
- **Terrorist Funds in your possession; and**
- **Economic Sanctions Reports (ESR).**

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

• Reporting Suspicious Transactions and Activities

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

i. that funds being used for the purpose of a transaction or attempted transaction are the proceeds of a criminal conduct *(See s.55A of the POCA)*;

ii. a transaction or an attempted transaction is related to the commission or attempted commission of a Money Laundering offence; or

iii. that funds being used for the purpose of a transaction or attempted transaction within the entity are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism *(See s.22C (3) of the ATA).*

iv. that funds being used for the purpose of a transaction or attempted transaction within the entity are linked or related to, or to be used for proliferation financing or that the transaction is being attempted by an entity or an associate of an entity listed on the list of entities in relation to proliferation financing. (See s.3(2) of the CPFA and regulation 5(4) of the CPFRs).

The STR/SAR must be submitted to the FIUTT within five (5) days of the date the transaction was **deemed** to be suspicious for a ML or predicate offence related suspicious transaction *(See S55A (3) of the POCA), immediately for a TF or PF related suspicious transaction (See s.22C of the ATA and s.5 of the CPFA)*

- *Defining Knowledge and Suspicion*

The first criterion above provides that, before you become obliged to report, you must **know** or **have reasonable grounds for suspecting,** that some other person is engaged in Money Laundering, Financing of Terrorism or Proliferation Financing.

If you actually 'know' that your client is engaged in Money Laundering, then your situation is quite straightforward – the first criterion is met.

Reasonable grounds to suspect

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

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

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

Attempted Transactions

If a client attempts to conduct a transaction, but for whatever reason that transaction is not completed, and you think that the attempted transaction is suspicious, you must report it to the FIUTT.

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

- *How to identify a Suspicious Transaction or Activity*

Determining whether a transaction or activity is suspicious is based on your knowledge of the customer and of the industry. You and your employees, if any, are better positioned to identify transactions which lack justification or do not fall within the usual methods of legitimate business. While there

may be general indicators of suspicious transactions, there are also indicators specific to the business of real estate which would help you and your employees to better identify suspicious transactions whether completed or attempted.

For examples of Suspicious Indicators as it relates to the TCSP Sector, see APPENDIX 2.

Other circumstances where a report must be made to the Compliance Officer for consideration to file an STR/SAR:

- Pursuant to regulation 4(2) of the CPFA, upon receipt of such report from the independent auditors of any suspicion or knowledge of a suspicious transaction or attempted suspicious transaction, the Compliance Officer shall consider whether he should submit a suspicious activity or suspicious transaction report to the FIUTT. In accordance with regulation 4(3) of the CPFA, where the Compliance Officer determines that the report should be submitted to the FIUTT, he shall do so immediately.
- Pursuant to Regulation 11(6) of the FORS, where the TCSP is unable to apply customer due diligence in accordance with regulation 11(5), the matter shall be reported to the Compliance Officer who shall consider whether a suspicious transaction or suspicious activity report should be filed with the FIUTT.
- Further, regulation 5(1) of the CPFA gives guidance on undertaking due diligence as it relates to PF (i.e. the screening of customers against the list of listed entities) and identifies the circumstance in which a suspicious transaction or activity report should be filed with the FIUTT.

It should be noted that it is a very serious contravention where a customer attempts to enter into a transaction, or continue a business relationship and the TCSP fails to cease continuation of the attempted transaction or business relationship or file a suspicious transaction or activity report with the FIUTT. You may be susceptible to an Administrative fine or summary conviction for such a contravention.

For further guidance on Reporting STRs/SARs as it relates to procedure and associated offences, **click here.**

- Terrorist Property/Funds Reporting

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

(a) United Nations Security Council Resolution (UNSCR) 1267/1989/2253 Sanctions List and United Nations 1988 Sanctions Committee List

(together referred to as the "List of Designated Entities" in accordance with section 2(1) of the ATA[3]); and

(b) Trinidad and Tobago Consolidated List of Court Orders (TFS);

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

(a) At the on-boarding stage; **and**

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

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

For Guidance on reporting Terrorist Property or Funds as it relates to the relevant form and procedure please click **here**.

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

The **Economic Sanctions** (Implementation of United Nations Resolution on the Democratic Republic of Korea) **Order, 2018** and the **Economic Sanctions** (Implementation of United Nations Resolution on the Islamic Republic of Iran) **Order, 2018** aim to prevent and disrupt the financing of the proliferation of weapons of mass destruction which constitutes a substantial threat to both domestic and international peace and security. The CPFA and CPFRs further outline the measures which must be taken by all Supervised Entities, including TCSPs, to ensure they identify and understand their PF risks and that they implement mitigating measures commensurate with the risks identified.

Click here for Guidance On A Risk Based Approach To Counter-Proliferation Financing For Reporting Entities

The up-to-date list of entities listed in accordance with the DPRK and Iran Orders can be found on the website of the Anti-Terrorism Unit, Office of the Attorney General.

Pursuant to these Orders and the CPFRs, you are required to **IMMEDIATELY** inform the FIUTT, when the Attorney General circulates the list of entities which have been

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

the subject of a freezing Order by the Supreme Court of Judicature of Trinidad and Tobago, of the following circumstances:

1. Where you have knowledge or reasonably suspect that any entity named in the Court Order has property or funds within your business;

2. Where a transaction is being conducted by a person involving property or funds owned or controlled, whether directly or indirectly, by an entity named in the Court Order

These reports are to be submitted to the FIUTT using an **Economic Sanctions Reporting Form** (ESR).

For further guidance on Submitting ESRs as it relates to obligations, procedure and associated offences, **click here.**

IX. RECORD KEEPING

As a supervised entity you are required to retain records, including those related to transactions and client identification, for a period of six (6) years in electronic or written form. Retention of these records and the exercise of proper record keeping practices enable you to comply with lawful requests for information from auditors, other competent authorities and law enforcement authorities that request these records for the purposes of criminal investigations or prosecutions (*See Regulation 31 of the FORS and section 4 of the CPFA).*

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

[Intentionally left blank]

4. GENERAL OFFENCE FOR FAILURE TO COMPLY WITH REGS AND FORS

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

Contravention of the POCA

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

Contravention of the FORS

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

Contravention of the FIUTT Regulations

Where a FI or LB commits an offence under the FIUTT Regulations where no penalty is specified, it shall be liable on summary conviction, to a fine of five hundred thousand dollars and to a further fine of twenty-five thousand dollars for each day that the offence continues; and on conviction on indictment, to a fine of one million dollars and to a further fine of fifty thousand dollars for each day that the offence continues. *(See section 27 of the FIUTTA and Regulations 36 and 37 of the FIUTT Regulations)*

Contravention of the ATA

A FI or LB which fails to comply with Section 22AB or Section 22C (1), (2) or (3) of the ATA commits an offence and is liable a) on summary conviction to a fine not exceeding two million dollars and imprisonment for a term not exceeding two years; or (b) on conviction on indictment to a fine not exceeding five million dollars and imprisonment for a term not exceeding seven years *(See Section 42(1) of the ATA)*.

Where a company commits an offence under Section 22AB or Section 22C (1), (2) or (3) of the ATA, any officer director or agent of the company who directed, authorised, assented to, or acquiesced in the commission of the offence or to whom any omission is attributable, is a party to the offence

and is liable in summary conviction or conviction on indictment in the same manner as the above paragraph. *(See Section 42(2) of the ATA).*

Contravention of the ATA Regulations

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

Contravention of the CPFA

An FI or LB which fails to comply with Section 5 or Section 9 of the CPFA commits an offence and is liable on summary conviction to a fine not exceeding two million dollars and to imprisonment for a term not exceeding two years and on conviction on indictment, a fine not exceeding five million dollars and imprisonment for a term not exceeding seven years. (See Section 12 of the CPFA)

Where a company commits an offence under the CPFA, any officer director or agent of the company who directed, authorised, assented to, acquiesced in or participated in the commission of the offence is a party to, and commits the offence and is liable on conviction to the punishment provided for the offence.

Contravention of the CPF Regulations

An FI or LB which does not comply with the ATA Regulations commits an offence and is liable on summary conviction to a fine not exceeding two million dollars and to imprisonment for a term not exceeding two years, or on conviction on indictment to a fine not exceeding five million dollars and to imprisonment for a term not exceeding seven years (See Section 12 of the CPFA).

ADMINISTRATIVE FINES

Contraventions of the FORs, FO(FT)Rs, FIUTTRs or CPFRs can result in the imposition of an Administrative Fine (see section 57 of the POCA, section 42 of the ATA, section 27 of the FIUTTA and section 12 of the CPFA). Notwithstanding the above, the FIUTT recognises that it is the general nature of its Supervised Entities to cooperate and comply once contraventions are identified. In this vein, it is expected that an Administrative Fine will only be pursued in exceptional circumstances short of circumstances warranting criminal action or where multiple attempts at bringing the entity into compliance have proved futile.

[Intentionally left blank]

APPENDIX 1 - CASE STUDIES

Case 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.

Case 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 funneling 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: FATF Report 2010 – Money Laundering using Trust and Company Service Providers

[Intentionally left blank]

APPENDIX 2 - AML/CFT/CPF SUSPICIOUS INDICATORS FOR TCSPs

While general indicators may point to a suspicious transaction, industry-specific indicators would also help you and your employees to better identify suspicious transactions whether completed or attempted.

Consider the following red flags:

- your customers including professional intermediaries are evasive or reluctant to provide required CDD information or documentation;
- you are advised that ownership information is confidential;
- requests from professionals to provide services to their customers that can be used as part of a scheme to disguise income, assets, and ownership;
- you are asked to provide services that assist in the establishment of multi-jurisdictional and/or complex structures with no commercial rationale;
- you are asked to provide multiple companies or trusts that add unnecessary layers of complexity;
- you are offered an excessive fee for the level of services provided;
- the number of intermediaries or professionals in the supply chain seems excessive;
- excessive or unnecessary use of nominees;
- intermediary chains where service providers are asked to act as nominee directors for large numbers of limited companies;
- intermediary chains where service providers market themselves and their jurisdictions as facilitating anonymity and disguised asset ownership;
- offshore bank accounts being used with no apparent legitimate economic requirement and where sources and/or destinations of funds are unknown;
- being asked to provide services to a company whose primary purpose is collecting funds from various sources for transfer to local or foreign bank accounts with no apparent ties with the company;
- you identify large movements of funds through a customer's company with no apparent legal or commercial reason and an absence of any underlying transactions;
- you note funds being transferred in the form of "loans" to individuals from trusts and non-bank shell companies, facilitating a system of regular transfers to these corporate vehicles from the individual recipients of the loans, in the form of repayments;
- your customers are native to, resident in, or incorporated in a higher-risk country;
- the money flow generated by a company is not in line with its underlying business activities;
- the beneficial owners are located in offshore jurisdictions or high risk third countries, or countries with high levels of corruption, illicit drug dealing or organised crime; and
- the purchase of companies that have no obvious commercial purpose companies which continuously make substantial losses.

Source: UK Government – *"Trust or company service provider guidance for money laundering supervision,* Trust or company service provider guidance for money laundering supervision - GOV.UK (www.gov.uk) *"*

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

-END OF DOCUMENT-