



GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO



FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO

Ministry of Finance

CUSTOMER DUE DILIGENCE GUIDANCE TO SUPERVISED ENTITIES

UPDATED JULY, 2025

Purpose

This Guidance is intended to provide assistance to Non-Regulated Financial Institutions and Listed Businesses (collectively "Supervised Entities") supervised by the Financial Intelligence Unit of Trinidad and Tobago

FIUTT REFERENCE: GN/001/2025

Table of Contents

List of abbreviations and acronyms	3
1. INTRODUCTION AND PURPOSE	4
1.1 WHAT ARE CDD MEASURES?	4
1.2 WHEN IS CDD REQUIRED?	4
2. RISK BASED APPROACH TO CDD	6
2.1 GENERAL CDD REQUIREMENTS.....	6
2.1.1 Identification of the customer	7
2.1.2 Verifying the identity of a customer	7
2.1.3 How do I identify a child?.....	8
2.2 SIMPLIFIED DUE DILIGENCE	9
2.2.1 Examples of SDD measures.....	9
2.3 ENHANCED DUE DILIGENCE	11
2.3.1 Examples of EDD measures.....	11
3. SPECIFIC CDD MEASURES.....	13
3.1 INDIVIDUALS (NATURAL PERSONS)	13
3.2 LEGAL PERSONS	13
3.2.1 Identify and verify the identity of the legal person, its legal status, the nature of its business and the source of funds for the business relationship or transaction.	14
3.2.2 Identify and verify the identity of directors and other officers of a company, partners of a partnership, account signatories and sole traders using reliable source documents.....	15
3.2.3 Beneficial Ownership.....	15
3.2.4 Ensure that persons purporting to act on behalf of the business entity or company are authorised to do so.....	16
3.2.5 Customers who are Non-Profit Organisations.....	16
3.3 TRUSTEES, NOMINEES OR OTHER LEGAL ARRANGEMENTS.....	17
3.3.1 Identifying and verifying the identity of the customer	17
3.3.2 Beneficial Ownership.....	18
3.4 NON FACE-TO-FACE CUSTOMERS.....	18
3.5 FOREIGN CUSTOMERS (NON-RESIDENT)	19
3.6 POLITICALLY EXPOSED PERSONS (PEPS)	20
4. USING A THIRD PARTY TO VERIFY CUSTOMER IDENTITY	21
4.1 RELIANCE ON A THIRD PARTY FINANCIAL INSTITUTION OR LISTED BUSINESS LOCATED IN ANOTHER JURISDICTION.....	21

4.2 RELIANCE ON A THIRD PARTY FINANCIAL INSTITUTION OR LISTED BUSINESS IN THE SAME GROUP	21
5. Ongoing Due Diligence	23
5.1 ONGOING MONITORING OF CUSTOMER TRANSACTIONS	23
6. WHO SHOULD NOT BE DEALT WITH AS CUSTOMERS?.....	24

List of abbreviations and acronyms

ABBREVIATION	MEANING
AML/CFT/CPF	Anti-Money Laundering/Counter Financing of Terrorism/Counter Proliferation Financing
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution
FIUTT	Financial Intelligence Unit of Trinidad and Tobago
FOR	Financial Obligations Regulations, 2010
LB	Listed Business
ML/FT/PF	Money Laundering/Financing of Terrorism/Proliferation Financing
NPOs	Non-Profit Organisations
PEP	Politically Exposed Person
PF	Proliferation Financing
RBA	Risk Based Approach
SDD	Simplified Due Diligence
STR/SAR	Suspicious Transaction Report/Suspicious Activity Report
UN	United Nations

1. INTRODUCTION AND PURPOSE

This Guidance is intended to provide assistance to Non-Regulated Financial Institutions and Listed Businesses supervised by the Financial Intelligence Unit of Trinidad and Tobago (“FIUTT”) (“Supervised Entities”) in complying with their legal obligations for conducting customer due diligence (“CDD”).

The Financial Obligations Regulations 2010 of Trinidad and Tobago (“the FORs”), particularly Part III of the FORs, sets out the necessary approach to CDD which Supervised Entities must follow when entering into a business relationship with a customer and when conducting business transactions with customers.

The FORs require that Supervised Entities apply a Risk Based Approach (RBA) to determine the extent of the CDD measures which should apply to particular customers in certain circumstances. This Guidance seeks to ensure that comprehensive customer identification information is appropriately acquired and verified; and that customers’ transactions are monitored in accordance with the Supervised Entity’s RBA.

This Guidance is a general, informative document and is not intended to replace the FORs or any of the 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.

1.1 WHAT ARE CDD MEASURES?

CDD relates to the identification and verification of persons and entities with whom a Supervised Entity intends to conduct business. CDD consists of five (5) parts:

1. Customer identification and where applicable, identification of the customer’s beneficial owner or authorised agent;
2. Verification of the customer’s identity, beneficial owner or authorised agents identity;
3. Understand and, as appropriate, obtain information on the nature and purpose for which the customer intends to conduct business with the Supervised Entity;
4. Identification and, as appropriate, verification of the Source of Funds with which the customer intends to conduct the business transaction with the Supervised Entity; and
5. Conduct ongoing due diligence on the business relationship and scrutinise transactions throughout the relationship.

1.2 WHEN IS CDD REQUIRED?

The purpose of the CDD process is to ensure that Supervised Entities know their customers and understand the nature of their business relationship with the Supervised Entity. CDD should be conducted on the customer and, where applicable, the beneficial owner, and the person acting on behalf of the customer.

In accordance with Regulation 11 of the FORs, CDD should be conducted at the following times:

1. **Before** establishing a business relationship;
2. **Before** completing a one-off or occasional transaction of fifty thousand Trinidad and Tobago dollars (TT\$50,000.00);
3. **Before** completing two or more one-off transactions which are each less than of fifty thousand Trinidad and Tobago dollars (TT\$50,000.00), but together the total value is TT\$50,000.00 or more, and it appears that the transactions are linked;
4. **Before** undertaking a one-off or occasional wire transfer of six thousand dollars (\$6,000) or more; and
5. **Before** undertaking two or more wire transfers of less than six thousand dollars (\$6,000) each, but together the total value is six thousand dollars (\$6,000) or more and it appears that the transactions are linked.

Supervised Entities who are members clubs registered under the Registration of Clubs Act and licensed under the Gambling and Betting Act have a specific obligation to conduct CDD when their customers engage in:

1. *A transaction of **TT\$10,000.00** and over; or*
2. *Two or more transactions, each of which is less than **TT\$10,000.00** but together the value amounts to **TT\$10,000.00 or more**, and it appears, either at the outset of each transaction or subsequently, that the transactions are linked.*

Supervised Entities should also conduct CDD where:

1. There is suspicion of ML/FT, regardless of the amount of the transaction, unless doing so results in tipping off the customer. In such instances, the Supervised Entity may forego the CDD and must file an STR/SAR in accordance with Regulation 11(8) of the FORs.
2. There is doubt about the veracity and adequacy of documents, data or information previously obtained for the purposes of identification or verification;
3. There is a change in the circumstances of the customer, for example, changes to the customer's transaction activity.

To this end, Supervised Entities are required to have a written customer acceptance policy, included in the compliance programme, outlining the procedures to be followed in determining whether to establish a business relationship or complete a transaction.

2. RISK BASED APPROACH TO CDD

Supervised entities are required by Regulation 7(2) of the FORs to take appropriate steps to identify, assess and understand their ML/FT/PF risks for customers, and what measures are to be taken to manage and mitigate such risks. As a result, Supervised Entities are required to develop and implement risk based policies and procedures to mitigate the ML/FT/PF risks identified in their customer risk assessments. Risk Based policies should be aligned with the [National Risk Assessment](#) and any other risk assessment, whether sectoral or thematic, published by a competent authority.

Based on the RBA, the risk assessment framework should be used to identify which customers or categories of customers present higher or lower risks in order to determine the level of CDD measures required. Where a customer is assessed by the Supervised Entity as being low risk, [Simplified Due Diligence \(“SDD”\) measures](#) should be applied. Whereas, where the customer is assessed as being high risk, the Supervised Entity must apply [Enhanced Due Diligence \(“EDD”\) measures](#).

It is important to note, however, that where SDD and EDD measures are applied by the Supervised Entity the CDD policies and procedures should clearly state the rationale and the applicable measures to be undertaken when applying each.

For further information on the implementation of a Risk Based Approach to AML/CFT/CPF please see the FIUTT’s [Guidance on implementing a Risk Based Approach](#).

2.1 GENERAL CDD REQUIREMENTS

In keeping with a RBA, Regulation 15 of the FORs sets out the general CDD requirements which should be applied to all customers of the Supervised Entity. These requirements may be simplified or enhanced depending on the risks identified for each customer.

General customer identification and verification measures refer to obtaining the following types of information from a customer:

1. The customer’s full name (his/her given/legal names);
2. The customer’s permanent residential address;
3. The date of birth of the customer;
4. The customer’s nationality;
5. The customer’s business or occupation, where applicable (i.e. in circumstances where the customer is employed);
6. The customer’s occupational income, where applicable (i.e. in circumstances where the customer received an income from his occupation/employment);
7. The customer’s signature;
8. The purpose and intended nature of the new business relationship or the transaction being carried out;
9. Source of the funds being used to establish the business relationship or conduct the transaction; and

10. Any other information which the Supervised Entity may deem appropriate depending on its policies.

Record Keeping

It is important to note that Regulation 31 of the FORS requires a Supervised Entity to keep records of all identification data obtained through the customer due diligence process. This data must be kept in electronic or in written form and for a period of six years. It enables the Supervised Entity to provide lawfully requested information to auditors, competent authorities and law enforcement agencies for the purpose of criminal investigation or prosecution. For more information please see the FIUTT's [Guidance on Record Keeping Requirements](#).

2.1.1 Identification of the customer

It is important to distinguish between identifying the customer and verifying identification. Customer identification entails the gathering of information on the prospective customer to enable identification and includes for example, obtaining information on his/her given/legal name, residential address, nationality, date and place of birth. For customers who are [legal persons](#) or [legal arrangements](#), the appropriate adaptations shall apply.

2.1.2 Verifying the identity of a customer

Verification of the customer identity entails checking reliable, independent source documentation that confirms the veracity of the information obtained during the CDD process. Simply put, the Supervised Entity must satisfy itself that it is certain of the identity of its client using the best available information. Supervised Entities should be aware that the best documents for the verification of identity are those most difficult to obtain or counterfeit.

Verifying identity is a crucial element of the AML/CFT/CPF regime of Trinidad and Tobago as it helps the Supervised Entity to know its clients and to understand and assess any risk that may be associated with their transactions or activities.

2.1.2.1 Reliable source information

Supervised Entities should verify the identity of its customers using at least one (1) original form of reliable source information. Reliable source information may include, but is not limited to the following types of government issued identification documents:

1. Valid National Identification Card;
2. Valid Passport;
3. Valid Drivers' Permit;
4. Birth Certificate only to confirm date and place of birth;

5. Utility bills excluding mobile phone bills, tax assessment, account statement from a financial institution, letter from a public authority, to confirm address provided. Where the utility bill is not in the customer's name, the Supervised Entity should request additional information to confirm the customer's address such as obtaining a letter from the landlord or a copy of the lease agreement and a recent receipt. ***(Please note that this list is not exhaustive).***

Where original documents are not available, copies shall only be accepted where they are certified by identification, in accordance with Regulation 15(4) of the FORs.

N.B. The following are not an acceptable source of information to verify a person's identity:

- Identification documents which do not bear photographs or signatures;
- Social media; and
- A Post Office Box number is not an acceptable address.

It is important to note that Regulation 31 of the FORS requires a Supervised Entity to keep records of all identification data obtained through the customer due diligence process. This data must be kept in electronic or in written form and for a period of six years. It enables the Supervised Entity to provide lawfully requested information to auditors, competent authorities and law enforcement agencies for the purpose of criminal investigation or prosecution. See [Guidance on Record Keeping Requirements](#).

2.1.2.2 What if a person is unable to present a reliable source of information?

Some flexibility could be given to certain classes of clients (such as the elderly, the disabled, students and minors) who may not be able to produce the usual types of evidence of identity such as a driver's license, passport or ID card. However, in those circumstances the flexibility given should not sufficiently compromise the AML/CFT/CPF procedures recommended in this document.

If the Supervised Entity is unable to obtain adequate information to satisfy itself of the identity of the customer, or where the customer identity cannot be verified, the Supervised Entity must report the matter to its Compliance Officer and discontinue any business relationship with the customer.

Supervised Entities are prohibited from conducting business with or opening accounts for anonymous customers or customers with fictitious names.

2.1.3 How do I identify a child?

If a child is under 12 years of age, you must verify the identity of one parent or guardian and record the parent or guardian information. You can rely on the information provided by the parent or guardian and the child's birth certificate in order to record the child's identification details.

If a child is between 12 and 15 years of age, and has a passport you may be able to use it to verify their identity. If not, you could rely on the parent's driver's licence to verify the parent's name and their common address, and the child's birth certificate to verify the child's name and date of birth.

2.2 SIMPLIFIED DUE DILIGENCE

Simplified Due Diligence (SDD) represents the most basic tier of due diligence, applied when initiating a business relationship or transaction with a customer deemed low risk. It empowers Supervised Entities to adopt a streamlined, proportionate approach—reducing the intensity of checks for low-risk scenarios while preserving full compliance with AML/CFT/CPF regulations. By so doing, SDD enables smarter resource allocation, allowing greater focus on higher-risk areas where scrutiny is most needed. Crucially, it introduces operational flexibility, ensuring that compliance remains dynamic and risk-sensitive—without overburdening processes where AML/CFT/CPF risks are minimal.

- ✓ ***Supervised Entities are encouraged to use SDD in low risk circumstances which align with the results of a [National Risk Assessment](#) or Sectoral/Thematic Risk Assessment conducted by the FIUTT or other competent authority.***
- ✓ ***SDD should only be applied where there are adequate systems in place to monitor customer transactions and changes in customer risk profiles.***
- ✓ ***SDD shall not be applied when there is a suspicion of ML/FT/PF or where risks are high.***

In accordance with Regulation 14 of the FORs, a Supervised Entity may apply SDD measures to obtain evidence of the identity of a person in any of the following circumstances:

- i. where the risks identified are lower;
- ii. where the Supervised Entity carries out a one-off transaction with an authorised agent of a customer who has been introduced to the Supervised Entity by a Listed Business (“LB”) or Financial Institution (“FI”), and the FI or LB has provided written assurance that evidence of the identity of the agent introduced by him has been obtained and recorded, and can be made available to the Supervised Entity on request (see [Third Party Reliance](#));
- iii. Where the customer is regulated by the Central Bank of Trinidad and Tobago or the Trinidad and Tobago Securities and Exchange Commission;
- iv. Where the customer is a public company listed on the Trinidad and Tobago Stock Exchange; and
- v. Where the customer is a public authority.

2.2.1 Examples of SDD measures

- a. Adjusting the quantity of information requested from the customer for identification, verification or monitoring purposes. Customers warranting SDD based on their risk profile may need to provide less documentation than is required for general CDD measures;
- b. Adjusting the quality or source of information obtained for identification, verification or monitoring purposes. For example, the use of student IDs for performing low risk transactions for verified students;

- c. Adjusting the frequency of CDD updates and reviews of the business relationship. Reviews and updates on lower risk customers can take place when trigger events occur and not as frequently as CDD or EDD measures require;
- d. Adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only.

The following are some practical examples of the application of SDD in low risk circumstances:

- A **real estate agent** facilitating the sale of a property to a publicly listed company in a low-risk jurisdiction (e.g., FATF-compliant country) may apply SDD.
 - **Why SDD applies:** The buyer is a regulated entity with transparent ownership and financial reporting.
 - **SDD Measures:** Basic identity verification of the company (e.g. Certificate of Incorporation) and confirmation of listing status.
- An **accountant** providing tax filing services to a salaried employee with a long-standing relationship and no complex financial activity.
 - **Why SDD applies:** Low risk of money laundering due to the nature of the client and service.
 - **SDD Measures:** Use of existing client records and limited additional verification.
- A **TCSP** setting up a company for a government-owned enterprise in a FATF-compliant country.
 - **Why SDD applies:** The client is a publicly owned entity with transparent ownership.
 - **SDD Measures:** Verification of government ownership and minimal ongoing monitoring.

Please note that the above are examples only and should not be construed as rules. Each situation and customer should be assessed on its own merits.

Where –

- (i) the aforementioned low risk circumstances exist;
- (ii) there are adequate systems in place to monitor customer transactions and changes in customer risk profiles; and
- (iii) there is no suspicion of ML/FT/PF

and the Supervised Entity chooses not to apply SDD, the Supervised Entity should document its rationale for not applying same.

2.3 ENHANCED DUE DILIGENCE

Generally, EDD measures require you to obtain further information, including additional evidence of identity, better forms of verification of identity, verification of the source of wealth and source of funds and in certain situations the permission of senior management before establishing the business relationship.

In particular, EDD must be applied:

- i. Where the risks identified are higher, such as in cases where the customer's business activities are cash intensive or include the purchasing of high value goods such as cars, jewellery and real estate;
- ii. Where the customer or Beneficial Owner is a Foreign or high risk [Politically Exposed Person \(PEPs\)](#);
- iii. Where the applicant for business acts or appears to act in a representative capacity (an agent of a principal);
- iv. Where the customer is not a resident of Trinidad and Tobago;
- v. Where the applicant for business acts or appears to act in a representative capacity (an agent) for a non-resident customer (his principal);
- vi. Where you know or suspect money laundering or terrorist financing;
- vii. In trusts and fiduciary relationships;
- viii. Where the customer comes from a jurisdiction considered to be high risk (e.g. [countries identified by the Financial Action Task Force \(FATF\) as High Risk or under increased monitoring](#); from a Country in which the production or transportation of illegal drugs maybe taking place, from a Country with known or suspected terrorist activities, etc.); and
- ix. In Non-face-to-face business relationships or transactions.

2.3.1 Examples of EDD measures

- a. Increasing the quantity of information obtained for CDD purposes and requesting additional documentary evidence and/or utilizing publicly available sources. A Supervised Entity may request additional information as to the customer's residential status, employment, salary details and other sources of income and critically observe the customer's negative media news, if any and where relevant;
- b. Understanding the customer's ownership and control structure to ensure that the risk associated with the relationship is well known. This may involve the Supervised Entity keeping abreast of any negative media news pertaining to the potential Customer;
- c. Understanding the intended nature of the business relationship and the reasons for intended or performed transactions. This may include the Supervised Entity obtaining information on the number, size and frequency of transactions that are likely to be conducted with the Customer and requesting the Customer's cash flow projections, business plans and copies of contracts with vendors etc.;
- d. Reviewing current financial statements of the Customer to understand all aspects of their current financial status;

- e. Conducting enhanced, ongoing monitoring of the business relationship, by increasing the number, timing and frequency of formal reviews; and
- f. Verifying the source of funds or source of wealth of the Customer which may include intrusive measures such as requesting pay slips, certified or audited financial statements, title deeds or proof of inheritance through copies of wills or Court Settlements and Orders appropriating wealth.

****Please note that this list is not exhaustive***

3. SPECIFIC CDD MEASURES

3.1 INDIVIDUALS (NATURAL PERSONS)

When entering into a business relationship or conducting a transaction with natural persons, the Supervised Entity must perform due diligence measures commensurate with the risk identified for the customer. For customers who are identified as neither high risk nor low risk, [general CDD information](#) should be obtained and verified.

Where higher risks are identified, [EDD measures](#) shall be performed and additional identity verification information should be obtained. Such additional information for *individuals* may include, but are not limited to:

1. Additional picture identification;
2. Any other names used (such as marital name, former legal name or alias);
3. Residency status;
4. Job letters to verify employment status and job position, where applicable; and
5. Verification of the source of the funds intended to be used by the customer for the transaction or to establish the business relationship (e.g. Receipts or salary statements);
6. Destination of funds passing through the account; and
7. Any other information which the Supervised Entity may deem appropriate depending on its policies.

Where low risks are identified, SDD measures may be performed in accordance with [section 2.2.1](#) above. Supervised Entities are reminded that SDD measures should only be used where there are adequate systems in place to monitor customer transactions and changes in customer risk profiles and that SDD should never be conducted where there is a suspicion of ML.

3.2 LEGAL PERSONS

The Financial Action Task Force (“FATF”) defines a ‘legal person’ as *“any entity other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This includes companies, bodies corporate and foundations, anstalt-type structures¹, partnerships or associations and other similar type entities.”*

In Trinidad and Tobago, the various types of legal persons which may be formed include:

¹ An Anstalt is a hybrid between a company limited by shares and a foundation. It has no members, participants or shareholders, differs from a company in that it has no duty to return profit, and differs from a trust in that it has no obligation to a beneficiary. Anstalt do have, however, a holder of the founder’s rights. The founder can be either a legal person or a natural person. Anstalt are a civil law creation and no direct common law analogue exists. Common law courts have tended to treat Anstalt that are “limited by shares”, as a company, and those without shares are sometimes treated as a constructive trust. Source: <https://en.wikipedia.org/wiki/Anstalt>.

- a. A sole proprietorship/sole trader, which is a simple form of business structure where the business is owned and operated by a single individual, and there is no legal distinction between the owner and the business;
- b. A partnership, which is defined as the relation which subsists between persons carrying on a business in common with a view of profit²;
- c. A company incorporated under the Companies Act, Chap 81:01³;
- d. A Non-Profit Organisation registered under the Non-Profit Organisations Act, 2019.

When establishing a business relationship or conducting a transaction with a customer that is a Legal Person, in accordance with Regulation 16 of the FORs, a Supervised Entity is required to obtain general CDD information, with adaptations which are appropriate for a legal person. Such appropriate adaptations are described below:

3.2.1 Identify and verify the identity of the legal person, its legal status, the nature of its business and the source of funds for the business relationship or transaction.

Information obtained should include:

- a. Registered name of the legal person⁴;
- b. Registered address;
- c. Country of Incorporation (for legal persons who are incorporated entities);
- d. A signed Director's Statement outlining the nature of the company's business; and
- e. Information on the purpose and intended nature of the Business relationship.

3.2.1.1 The registered name, address and country of incorporation of the legal person should be verified by obtaining, as appropriate:

- a. the Certificate of Incorporation, Certificate of Registration⁵, Certificate of Continuance;
- b. Articles of Incorporation;
- c. Partnership Deed; and
- d. A copy of the By-Laws, where applicable.

² Section 3(1), Partnership Act, Chap. 81:02

³ These include for profit companies which may be limited by shares, by guarantee or have unlimited liability; and external companies.

⁴ Supervised Entities should have regard to the fact that some sole traders may register a business name pursuant to the Registration of Business Names Act, Chap. 82:85. All partnerships are considered firms pursuant to section 6 of the Partnership Act, Chap 81:02 and some firms may also need to be registered pursuant to the Registration of Business Names Act, Chap 82:85.

⁵ The Certificate of Registration should be obtained from sole traders, firms and corporations registered pursuant to the Registration of Business Names Act, Chap 82:85

3.2.1.2 For verification of the source of funds to be used for the business relationship or transaction, Supervised Entities should request, as far as possible:

- a. the management accounts for the last three years for self-employed persons or legal persons in operation for more than three years; or
- b. three-year estimates of income for self-employed persons or legal persons in operation less than three years.
- c. in circumstances where management accounts cannot be obtained, the supervised entity should obtain other proof of the source of funds to be used in the transaction.

3.2.2 Identify and verify the identity of directors and other officers of a company, partners of a partnership, account signatories and sole traders using reliable source documents.

Information obtained should include:

- a. Names of Directors, Secretary and officers, partners or sole trader;
- b. Copies of identification documents for at least two (2) Directors and the authorized account signatories;
- c. Duly certified copies of Powers of Attorney or other authorities; and
- d. Evidence of the authority to enter into the business relationship if necessary (for example, a copy of the Board Resolution).

3.2.3 Beneficial Ownership

In addition to the above customer identification and verification measures, Supervised Entities are required, under Regulation 12 of the FORs, to identify the beneficial owners of customers who are legal persons. Once identified, the Supervised Entity must take reasonable measures to **verify the identity of beneficial owners.**

The Supervised Entity **MUST** obtain the identity of the natural person who ultimately controls and/or owns the Business Entity or Company. In some circumstances, the Business Entity or Company may have a complex ownership structure in that its shareholders or controllers are other multiple legal persons. The Supervised Entity must go as far as reasonably practicable to identify the natural person who ultimately controls and/or owns these other legal persons.

Once the identities of the beneficial owners are obtained the Supervised Entity is required to take reasonable measures to verify the identities of the beneficial owners using reliable source documents. For further information and examples of how to determine Beneficial Ownership of Legal Persons, please consult the FIUTT's [Beneficial Ownership Guidance for Supervised Entities](#).

3.2.4 Ensure that persons purporting to act on behalf of the business entity or company are authorised to do so.

Transactions carried out with or on behalf of legal persons will be initiated through representatives of the legal person. Supervised Entities must verify that any person purporting to act on behalf of the legal person is in fact authorised to do so. Supervised Entities are also required to obtain and verify the identity of the representative using reliable source documents.

Table 1- SUMMARY OF CDD MEASURES FOR LEGAL PERSONS

A. Obtain and verify the identity of the following NATURAL PERSONS, where applicable [Regulation 16(1)]:
Sole Traders
Directors
Officers of the company
Partners of a partnership
Account Signatories
Beneficial Owners
Shareholders holding more than 10% of the paid up share capital of the company
Any person purporting to act on behalf of the legal person (<i>authorization to act should also be obtained</i>)
B. Obtain the following information in relation to the LEGAL PERSON, where applicable [Regulation 16(2)]:
Certificate of Incorporation, Certificate of Registration or Certificate of Continuance
Articles of Incorporation
Copy of Bye-Laws
Management accounts for the last three years for self-employed persons or legal persons in operation for more than three years
Three-year estimates of income for self-employed persons or legal persons in operation less than three years
In circumstances where management accounts cannot be obtained, other proof of the source of funds to be used in the transaction

3.2.5 Customers who are Non-Profit Organisations

Non-Profit Organisations (“NPO”) customers are also subject to CDD requirements. Supervised Entities must apply a risk-based approach to CDD in accordance with the risk profiles of their NPO customers and should identify and verify the beneficial owners of the NPO customer, where applicable.

N.B. Supervised Entities are expected to treat NPOs as a regular customer, conduct due diligence based on the Supervised Entity’s assessment of the NPOs risk, and apply appropriate CDD, SDD or EDD on the NPO customer in accordance with the risk profile. Supervised Entities are encouraged to review the

[National Risk Assessment of Trinidad and Tobago](#) when considering the risk profile of their NPO customers.

Where the NPO is the customer of the Supervised Entity, there is *no regulatory requirement in the FORs nor is there a supervisory expectation for Supervised Entities to have unique, additional due diligence steps for NPOs or to conduct due diligence on the donors and beneficiaries of NPOs.* However, Supervised Entities should understand basic information on the types of donors and of beneficiaries receiving funds from NPOs, where it is applicable to the business relationship between the Supervised Entity and the NPO.

Supervised Entities who are NPOs should also consult the FIUTT's [Guidance to NPOs](#) for further information on risk and CDD requirements which are specific to its business type.

3.3 TRUSTEES, NOMINEES OR OTHER LEGAL ARRANGEMENTS

3.3.1 Identifying and verifying the identity of the customer

According to the FATF the term 'legal arrangement' refers to express trusts or other similar legal arrangements such as trustees and nominees. When establishing a business relationship with a customer that is a Trustee, a Nominee or other Legal Arrangement, the following information in Table 3 should be obtained.

Table 2– LEGAL ARRANGEMENTS – IDENTIFICATION INFORMATION

Minimum Information Requirements
Name of the legal arrangement and proof of existence
Address and country of registered office
Nature, purpose and objectives of the legal arrangement
The names of the settlor and the name of the person providing the funds if not the ultimate settler, the trustee(s), the protector/controller(s) (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement (including through a chain of control/ownership)
Description of the nature and purpose/activities of the legal arrangement
Expected use of the account as it relates to the amount, number, type, purpose and frequency of the transactions expected.

Supervised Entities should verify the identity of the customer through the information obtained in Table 2, using reliable source information as discussed in [section 2.1.2](#) above. In addition to the requirements outlined in Table 2, Supervised Entities should also obtain the following information in accordance with Regulation 17 of the FORs:

- i. Evidence that the person has been appointed Trustee or Nominee by means of a certified copy of the Deed of Trust or Nominee arrangement;
- ii. The nature and purpose of the trust;
- iii. Verification of the identity of the trustee, the protector and the settlor and any other natural person exercising ultimate effective control over the trust or other legal arrangement; and
- iv. Information on the identity of the beneficiary or class of beneficiaries and verification of this information where available.

The Supervised Entity should also ensure that the identity of a beneficiary of a trust or other legal arrangement is verified before the pay-out to the beneficiary or before the exercise of any vested rights.

3.3.2 Beneficial Ownership

In addition to the above customer identification and verification measures, Supervised Entities are required, under Regulation 12 of the FORs, to identify the beneficial owners of customers who are legal arrangements. Once identified, the Supervised Entity must take reasonable measures to verify the identity of *beneficial owners* using reliable source documents. For further information and examples of how to determine Beneficial Ownership of Legal Arrangements, please consult the FIUTT's [Beneficial Ownership Guidance for Supervised Entities](#).

3.4 NON FACE-TO-FACE CUSTOMERS

You may encounter situations where the customer does not present himself when conducting transactions. This may occur with services provided electronically. All guidelines identified above for face-to-face customers apply to non face-to-face customers but additionally, Supervised Entities must identify, and put policies in place to address, the specific concerns which may arise with non face-to-face business relationships or transactions.

The measures taken for verification of a customer's identity in respect of non face-to-face business relations with the customer will depend on the nature and characteristics of the product or service provided and the customer's risk profile.

The verification checks may include:

- i. Telephone contact with the customer at a residential or business number that can be verified independently;
- ii. Confirmation of the customer's address through an exchange of correspondence or other appropriate method;

- iii. Telephone confirmation of the customer's employment status with his/her employer's human resource department at a listed business number of the employer;
- iv. Confirmation of the customer's salary details by requiring the presentation of a recent job letter or bank statement, where applicable; or
- v. Provision of identification documents certified by relevant authorities, e.g. notaries public.

3.5 FOREIGN CUSTOMERS (NON-RESIDENT)

Supervised Entities may experience difficulty when verifying and authenticating the identification, source of funds and source of wealth of Foreign Customers thereby resulting in AML/CFT/CPF risks. Further, the implementation of the FATF Recommendations in the country to which the Foreign Customer belongs may also influence its risk.

A Supervised Entity should establish policies, procedures and processes that provide for sound due diligence and verification practices, adequate risk assessment of these foreign customers, as well as ongoing due diligence. Suspicious or unusual activities ought to also be reported to the FIUTT in accordance with the above.

In applying the appropriate CDD measures above, the Supervised Entity should ensure to:

- i. Gather sufficient information about the customer to understand fully the nature of the customer's business and to determine from publicly available information the reputation of the customer;
- ii. Determine that the customer has anti-money laundering and terrorist financing controls;
- iii. Determine that the customer is effectively supervised by the competent authority in its jurisdiction, including whether the customer has been subject to a money laundering or terrorist financing investigation or other regulatory action;
- iv. Consider whether approval from senior management should be required before establishing such a relationship; and
- v. Contact the appropriate persons in that country for satisfactory evidence⁶ of the identity of the customer before completing the transaction.

In addition to the above, the Supervised Entity may obtain a reference from the foreign customer's Bank.

Where there are concerns that the identification documents of the non-resident Customer may not be genuine, the Supervised Entity should contact the relevant embassy or consulate to obtain confirmation. A Supervised Entity may also verify a non-resident customer's identification by

⁶ "satisfactory evidence of identity" means— (a) in relation to an individual, evidence that is reasonably capable of establishing or does in fact establish that the applicant for business is the person whom he claims to be; and (b) in relation to a corporation or other business arrangement, evidence that the corporation or other business exists and evidence of the identity of its directors, partners or persons of like status in the business arrangement.

requesting official documents such as job letters confirming employment arrangements for individuals on a work permit.

Where satisfactory customer due diligence information under v. above has not been obtained, the Supervised Entity must not proceed with the business relationship or one off transaction and the matter is required to reported to the Compliance Officer who must consider whether a suspicious transaction or activity report shall be filed with the FIUTT.

3.6 POLITICALLY EXPOSED PERSONS (PEPS)

In addition to the measures outlined above, you should ensure that you have appropriate risk management systems to determine whether the customer, an account holder or beneficial owner is a politically exposed person (PEP) as defined in the FORs. Please see the [FIUTT's Guidance on PEPs](#) for further information on treating with a customer who is a PEP.

Deliberately Left Blank

4. USING A THIRD PARTY TO VERIFY CUSTOMER IDENTITY

According to Regulation 11(1B) of the FORs, Supervised Entities may rely on a third party financial institution or listed business to apply CDD measures in respect of the identification of a customer, identification of the beneficial owner and understanding the nature of the business, or to introduce the business, provided that such third party consents. In these circumstances however, it is important to note that, in accordance with Regulation 11(1C) of the FORs, the Supervised Entity would maintain the ultimate responsibility for customer due diligence measures and not the third party relied on.

Since the Supervised Entity will remain liable for any failure in the application of CDD measures it should be satisfied that the third party is of reputable character, integrity and reliability.

According to Regulation 11(1D) of the FORs, if the Supervised Entity chooses to rely on the third party, it must:

- i. immediately obtain the necessary information concerning identification of the customer, identification of the beneficial owner and understanding the nature of the business;
- ii. satisfy itself that the third party is regulated, or supervised or monitored and has measures in place for compliance with CDD and record keeping requirements in line with the FORs; and
- iii. that the third party is willing and able to provide copies of identification data and other relevant documentation relating to the CDD requirements without delay upon request.

Where the Supervised Entity is unable to acquire copies of identification and other relevant documentation relating to the CDD requirements in accordance with iii. above, the Supervised Entity is responsible for performing the CDD processes.

4.1 RELIANCE ON A THIRD PARTY FINANCIAL INSTITUTION OR LISTED BUSINESS LOCATED IN ANOTHER JURISDICTION

In accordance with Regulation 11(1E) of the FORs, where a third party financial institution or listed business is located in another jurisdiction, the Supervised Entity must consider whether the conditions in (ii) above are met and should take into consideration the level of risk associated with those countries.

4.2 RELIANCE ON A THIRD PARTY FINANCIAL INSTITUTION OR LISTED BUSINESS IN THE SAME GROUP

Supervised Entities may rely on third party financial institution or listed business that is part of the same group as the Supervised Entity to perform elements of customer due diligence. Regulation 11(1F) of the FORs provides guidance to the Supervisory Authority (in this case the FIUTT) when

determining whether the third party can in fact meet the requirements stated in regulations 11(1B) and (1D). These include where:

- i. the group applies customer due diligence and record-keeping requirements and programmes against money laundering;
- ii. the implementation of the customer due diligence and record-keeping requirements under paragraph (i) and the anti-money laundering programmes are supervised at a group-level by the FIUTT; and
- iii. any higher risk country (as identified on a FATF list as a country with strategic anti-money laundering deficiencies) is adequately mitigated by the anti-money laundering policies of the group.

Deliberately Left Blank

5. Ongoing Due Diligence

In accordance with Regulation 11(1G) of the FORs, Supervised Entities are also required to conduct ongoing due diligence on existing customers. This includes scrutinising transactions throughout the course of the relationship to ensure that the transactions being conducted are consistent with the Supervised Entity's knowledge of the customers, their business and risk profiles, including where applicable, the source of funds.

Supervised Entities must ensure that documents, data or information collected under the CDD process is kept up to date and relevant, by conducting reviews of existing records.

Ongoing due diligence is applied on the basis of risk. Supervised Entities are required to apply **enhanced ongoing due-diligence** measures for customers that present higher ML/FT/PF risk due to business activity, ownership structure, nationality, residence status, politically exposed status or other higher risk indicators.

5.1 ONGOING MONITORING OF CUSTOMER TRANSACTIONS

In addition to conducting ongoing due diligence, a Supervised Entity should take measures to closely monitor the transactions undertaken through the course of the business relationship, to ensure that the transactions being conducted are consistent with its knowledge of the customer, their business and risk profile including, where necessary, the source of funds.

If there is a change in the customer's risk profile, the Supervised Entity should conduct CDD as appropriate to the change in risk

Deliberately Left Blank

6. WHO SHOULD NOT BE DEALT WITH AS CUSTOMERS?

Supervised Entities must have monitoring systems in place to ensure that business transactions are not carried out:

- i. Where satisfactory evidence of identity has not be obtained (please see [section 2.1.2](#) above);
- ii. With shell banks. A shell bank is a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision;
- iii. With anonymous accounts (Please refer to [section 2.1.2.2](#) above); and
- iv. For Persons designated as terrorist entities by the [Security Council of the United Nations](#) and listed on the [Trinidad and Tobago Consolidated List of High Court Orders](#) pursuant to section 22AB of the Anti-Terrorism Act, Chap. 12:07.

Please consult the FIUTT's [Guidance to Financial Institutions and Listed Business on Terrorist Financing and Procedures for Reporting Terrorists' Funds](#).

End of Document