Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF)

GUIDELINES FOR THE SECURITIES SECTOR

Updated-February 27, 2026

Table of Contents

LIST OF ACRONYMS & ABBREVIATIONS

ACO	Alternate Compliance Officer
AML/CFT/CPF	Anti-Money Laundering / Countering the Financing of Terrorism / Countering the Financing of Proliferation of weapons of mass destruction (also used for Combating the Financing of Terrorism and Combating the Financing of Proliferation)
ATA	The Anti-Terrorism Act, Chap. 12:07
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
CO	Compliance Officer
DNFBP	Designated Non-Financial Business or Profession
EAR	External Audit Report
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIUTT	Financial Intelligence Unit of Trinidad and Tobago
FIUTTA	Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01
FOFTR	Financial Obligations (Financing of Terrorism) Regulations (made under the Anti-Terrorism Act Chap. 12:07)
FORs	Financial Obligations Regulations (made under section 56 of the Proceeds of Crime Act Chap. 11:27)
FSRB	FATF-Styled Regional Body
FT/TF	Financing of Terrorism/Terrorist Financing
GCO	Group Compliance Officer
IOSCO	International Organization of Securities Commissions
KYE	Know Your Employee
LB	Listed Business
ML	Money Laundering

ML/TF	Money Laundering and Terrorism Financing
NAMLC	National Anti-Money Laundering Committee
NRA	National Risk Assessment
NPO	Non-Profit Organisation
PEP	Politically Exposed Persons
PF	Proliferation Financing
POCA	Proceeds of Crime Act, Chap. 11:27
RBA	Risk-Based Approach
SA	Securities Act, Chap. 83:02
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
TTSEC	Trinidad and Tobago Securities and Exchange Commission

1. INTRODUCTION

1.1 The Trinidad and Tobago Securities and Exchange Commission (TTSEC) is governed by the Securities Act, Chap. 83:02 (SA) and is the designated authority for registering and regulating issuers of securities, broker-dealers, securities exchanges and other registrants. The TTSEC as a designated Supervisory Authority[1] for Anti-Money Laundering and Combating the Financing of Terrorism and Counter Proliferation Financing (AML/CFT/CPF) (under the Proceeds of Crime Act, Chapter 11:27), is required under section 6(l) of the SA, to ensure that its registered financial institutions (FIs)[2] comply with the AML/CFT/CPF legislation in relation to the prevention of money laundering (ML) and combating the financing of terrorism (CFT) and any other written law that is administered or supervised by the Commission.

1.2 TTSEC's AML/CFT/CPF Guidelines ("Guidelines") shall not be regarded as a statutory instrument or have the power of law, it shall serve as a guide on laws and regulations as mandated under Trinidad and Tobago's AML/CFT/CPF legislative framework. The Guidelines contain guidance for financial institutions ("Registrant") registered under section 51(1) of the SA and to clarify key aspects of the regulatory regime for Registrants within the securities industry. Under the AML/CFT/CPF legislative framework, Registrants have a range of responsibilities, including:

a. Appointing a Compliance Officer and/or an Alternate Compliance Officer.
b. Developing and maintaining a risk assessment and risk-based AML/CFT/CPF programme;
c. Customer identification and identity verification;
d. Beneficial Owner identification;
e. Enhanced customer due diligence;
f. Ongoing customer due diligence;
g. Suspicious transaction reporting;
h. Record keeping; and
i. Auditing and annual reporting.

[1] "Supervisory Authority" means the competent authority responsible for ensuring compliance by financial institutions and listed businesses with requirements to combat money laundering terrorism financing and proliferation financing.

[2] For purpose of these Guidelines, "financial institution" has the meaning as defined in section 2 of the Proceeds of Crime Act, Chapter 11:27 - *a person registered under section 51(1) of the Securities Act*. The term "Registrant" will also be used in these Guidelines, which is defined in the Securities Act, Chapter 83:02, *as a person registered or required to be registered under Part IV of the Act.*

1.3 The Proceeds of Crime Act, Chap. 11:27 (POCA) and Financial Obligation Regulations (FORs) require financial institutions to develop a risk assessment and compliance programme that describes policies, procedures and controls aimed at meeting minimum requirements, and that adequately manages and mitigates the risks of money laundering and financing of terrorism. A risk-based approach offers flexibility to Registrants to respond proportionately to identified risks, and a well-targeted and prioritised AML programme will deter ML/TF activity.

1.4 Furthermore, Regulation 14 of the FORs and Regulation 3(1) of the FOFTR are intended to assist Registrants with, inter alia, complying with Trinidad and Tobago's AML/CFT/CPF laws and obligations, including applying a risk-based approach, through:

a. Understanding and complying with AML/CFT/CPF legislative and regulatory requirements;
b. Developing and implementing effective, risk-based AML/CFT/CPF compliance programmes that enable adequate monitoring, identification and reporting of suspicious transactions; and
c. Understanding the expectations of TTSEC with respect to the minimum standards for AML/CFT/CPF controls.

1.5 The risk-based approach, which is discussed more thoroughly in later sections, underpins the current regulatory regime. Registrants are expected to make decisions about how to identify, manage and mitigate ML/TF/PF risks according to the size, nature and complexity of the organisation.

1.6 The Guidelines seek to better inform Registrants of the need to implement effective policies and procedures to comply with the national AML/CFT/CPF legislative framework and to provide the securities sector with benchmarks for the proper functioning of their operations and will be referenced by the TTSEC in the conduct of its supervisory function. Furthermore, guidance will assist Registrants in determining how they may deal with meeting their obligations under the AML/CFT/CPF legislative framework.

1.7 Section 146(3) of the SA provides that contravention of a Guideline shall not prevent the TTSEC from acting under section 90 of the SA. In accordance with section 90(1)(c), where a compliance review conducted under section 89 or any other review or inspection reveals a

registrant is contravening or about to contravene the Act, Bye-laws or Guidelines under the POCA or any other AML law, the TTSEC may direct the Registrant within such time as may be specified, to take all such measures it may consider necessary to remedy the situation or minimise the prejudice.

1.8 The TTSEC notes that some Registrants are dually registered with the Central Bank of Trinidad and Tobago (CBTT). Notwithstanding this, dually registered entities are required to comply with the Guidelines when engaging in securities activities for which they are registered under the SA and comply with any joint guidance issued by the supervisory authorities.

2. INTERNATIONAL INITIATIVES

2.1. The Financial Action Task Force (FATF) is an intergovernmental body, and its objective is to set standards and promote effective implementation of legal, regulatory and operational measures for combating ML, TF, PF, and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations (The FATF Forty Recommendations), Guidance and Best Practices Papers to assist countries in implementing the Recommendations. These are recognised as international standards for combatting ML, TF and PF. The FATF Recommendations form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field. In order to ensure full and effective implementation of its standards at the global level, the Caribbean Financial Action Task Force (CFATF) (a FATF-style regional body), monitors compliance by conducting evaluations on jurisdictions and undertakes stringent follow-up after the evaluations, including identifying high risk and other monitored jurisdictions which could be subject to enhanced scrutiny by the FATF or counter-measures by the FATF members and the international community at large. Trinidad and Tobago is a member of the CFATF and is obliged to implement the FATF AML/CFT/CPF Recommendations.

3. PURPOSE AND SCOPE

3.1 The Guidelines for the Securities Sector are issued pursuant to Section 146 (1) of the SA and intended to provide guidance to Registrants (registered under section 51 of the SA), within the Securities Sector, in understanding their AML/CFT/CPF obligations under the legal and regulatory framework in force in Trinidad and Tobago.

3.2 The Guidelines set out the expectations of the TTSEC regarding the factors that entities within the sector should consider when identifying, assessing and mitigating the risk of ML, TF and PF. Entities should implement robust AML/CFT/CPF frameworks that are commensurate with their size, complexity and risk profile.

4. LEGISLATIVE FRAMEWORK

4.1 The AML/CFT/CPF legislative framework of Trinidad and Tobago comprises the following key laws:

a. The Proceeds of Crime Act and Regulations, Chapter 11:27;
b. The Anti-Terrorism Act and Regulations, Chapter 12:07;
c. The Financial Intelligence Unit of Trinidad and Tobago Act and Regulations, Chapter 72:01;
d. The Economic Sanctions Act, Chapter 81:05 and Orders issued thereunder; and
e. The Counter-Proliferation Financing Act, Act No. 8 of 2025

5. LEGAL STATUS

5.1 Section 146 (1) (c) of the SA provides that the TTSEC in consultation with the Minister may issue Guidelines on any matter it considers necessary to aid compliance with the Proceeds of Crime Act (POCA), the Anti-Terrorism Act (ATA) and the Economic Sanctions Act (ESA) or Orders made thereunder as they relate to PF, any other written law in relation to the prevention of ML, CFT, CPF or any other written law which may be administered or supervised by the Commission which may be in force from time to time.

5.2 The Guidelines are not intended to limit or otherwise circumscribe additional or supplementary guidance, circulars, notifications, memoranda, communications, or other forms of guidance or feedback, whether direct or indirect, which may be published on occasion by the TTSEC. As such, the Guidelines do not constitute additional legislation or regulation, and are not intended to set legal, regulatory, or judicial precedent. They are intended to be read in conjunction with the relevant laws and regulations currently in force in Trinidad and Tobago and do not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between the Guidelines and the legal or regulatory frameworks currently in force, the latter will prevail. Specifically, nothing in the Guidelines should be interpreted as providing any explicit or implicit guarantee or assurance that the TTSEC or other Competent Authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws and regulations.

5.3 The Guidelines and any lists and/or examples provided in them are not exhaustive and do not set limitations on the measures to be taken by institutions within the Securities Sector to meet their statutory obligations under the legal and regulatory framework currently in force. As such, the Guidelines should not be construed as legal advice or legal interpretation. Registrants should perform their own assessments of the manner in which they should meet their statutory obligations, and they should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to their particular circumstances.

5.4 It is the TTSEC's intention to update or amend the Guidelines from time to time, as and when it is deemed appropriate. However, Registrants should, as part of their risk management practices, stay current with emerging developments related to AML/CFT/CPF and update their AML/CFT/CPF Programmes as necessary. Registrants are reminded that the Guidelines are not the only source of guidance on the assessment and management of ML/TF/PF risk and that other bodies, including international organisations such as FATF, CFATF, and other FATF-style regional bodies (FSRBs), Basel, the Egmont Group and others also publish information that may be helpful in carrying out their statutory obligations. It is the sole responsibility of Registrants to keep appraised and always updated regarding the ML/TF/PF risks to which they are exposed, and to maintain appropriate risk identification, assessment

and mitigation programmes and to ensure their responsible officers, managers and employees are adequately informed and trained on the relevant policies, processes and procedures.

6. GENERAL DESCRIPTION OF MONEY LAUNDERING (ML) AND TERRORISM FINANCING (TF) AND PROLIFERATION FINANCING (PF)

Money Laundering

6.1 The goal of most criminal activity is to generate a profit for those who commit the criminal acts. ML is the process used to disguise the illicit source of the profit, i.e. money or assets, derived from criminal activity (Section 45 (1) of the Proceeds of Crime Act, Chap. 11:27 defines the money laundering offence). Once these proceeds are successfully 'laundered', a person is able to enjoy these funds without revealing the original source. Money laundering can take place in various ways.

6.2 There are three stages of money laundering:

a. **Placement**: this is the point at which the illicitly gained funds or assets enter the financial system. Placement generally occurs in the financial sector when the "dirty" funds are deposited directly into bank accounts and may even occur through the use of the funds to purchase financial instruments;

b. **Layering**: this is the point at which the illicitly gained funds are moved from the point of placement through the financial system in an effort to distance the funds from their illicit origin; and

c. **Integration**: this is the final stage of money laundering. After successful placement and layering of the illicitly gained funds, the funds now acquire a legitimate appearance and are then re-entered into the economy as "clean" money.

6.3 Money laundering is often considered to be associated with the activities of banks and money changers. However, securities market intermediaries, are also susceptible to money laundering activities. Whilst traditional securities market offers a vital laundering mechanism, particularly in the initial conversion of cash to stock, securities market investment schemes are one of the most attractive vehicles to the launderer.

6.4 While the securities sector (except for Collective Investment Schemes) may not generally accept cash for transactions, which is ordinarily the stage at which placement would occur, it is at risk for layering of these illicit funds. Illicit funds may also be generated from within the sector through fraudulent practices such as market manipulation and insider trading. The further movement of the profit from these criminal activities within the sector would constitute a money laundering offence.

Financing of Terrorism

6.5 Terrorism is the unlawful threat of action designed to compel the government or an international organisation or intimidate the public or a section of the public for the purpose of advancing a political, religious or ideological belief or cause.

6.6 Financing of terrorism is defined as the wilful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds will be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts. Terrorist financing requirements fall into two general areas:

(1) funding specific terrorist operations, such as direct costs associated with specific operations; and

(2) broader organisational costs to develop and maintain an infrastructure of organisational support and to promote the ideology of a terrorist organisation.

6.7 Unlike money laundering, terrorism financing is not usually committed with the goal of making a profit. The funds for Terrorist Financing may not only come from illicit sources but from legitimate means. Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

Proliferation Financing / Proliferation of Weapons of Mass Destruction

6.8 The FATF provides a broad working definition for proliferation financing (PF): "the act of *providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations*."

6.9 PF poses a significant threat to global security and unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organisations or acting as representatives or middlemen.

6.10 Proliferation of Weapons of Mass Destruction (WMDs) can take many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles).

7. PART 1: INTERNAL POLICIES AND PROCEDURES

The Role of the Board and Senior Management for the Oversight of the AML/CFT/CPF framework:

7.1 The Board of Directors has ultimate responsibility for the effective implementation of the Registrant's AML/CFT/CPF framework. Section 45 of the POCA establishes that a financial institution (FI) commits an offence of money laundering where the FI fails to take reasonable steps to implement or apply procedures to control or combat money laundering in accordance with the Regulations made pursuant to section 56 of the POCA. Depending on the size of the Registrant and other factors, oversight may fall within the remit of the Board or a sub-committee of the Board. In instances where a Registrant's corporate structure is such that no Board exists, senior management is expected to have oversight of the AML/CFT framework.

7.2 Registrants must implement an AML/CFT/CPF framework as part of their overall risk management strategy. ML, TF and PF expose a Registrant to transactional, compliance and

reputational risk and therefore an effective AML/CFT/CPF programme must be established, that minimizes these risks and potential costs.

7.3 A registrant, in accordance with Regulation 3 of the FORs, is to designate a manager or official employed at a managerial level as the Compliance Officer of that institution. The Registrant would be required to ensure that the CO can act independently of all other units and management to avoid conflicts of interest and influence. The Commission would, thereafter, approve the Compliance Officer based on the nature and complexity of the institutions and the risk posed thereto. An Alternate Compliance Officer should be designated to act in the absence of the Compliance Officer to discharge the functions of the Compliance Officer.

7.4 Section 22A of the ATA establishes the circumstances by which the offence of financing of terrorism may be determined. The Board has an oversight role designed to ensure inter alia, that there is compliance with all the relevant laws and international standards. Such compliance must assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

7.5 It is a requirement for a Registrant's Board of Directors to receive AML/CFT/CPF training at least annually. Such training is intended to, *inter alia*, improve the Board's knowledge of the subject matter and enhance the Board's effectiveness in overseeing the AML/CFT/CPF framework. In addition to the training received, the Board should supplement its knowledge of AML/CFT/CPF and the Registrant's AML/CFT/CPF framework by requesting from the Compliance Officer periodic briefings and/or reports, which detail:

a. The AML/CFT/CPF legislative and regulatory framework that apply to the Registrant's operations;
b. The AML/CFT/CPF framework adopted by the Registrant; and
c. The personnel across the various lines of business who are accountable for ensuring that the policies and procedures of the AML/CFT/CPF framework are adopted and followed.

7.6 Under Regulation 43 of the FORs, where a company commits an offence, any officer, director or agent of the company—

(i) who directed, authorised, assented to, or acquiesced in the commission of the offence; or

(ii) to whom any omission is attributable, is a party to the offence and is liable on summary conviction or on conviction on indictment, to the penalty prescribed in Section 57 of the Act, whether or not the company has been prosecuted or convicted.

7.7 Directors and senior management must be aware that:

a. The use of a group wide policy does not absolve Directors of their responsibility to ensure that the policy is appropriate for the Registrant and compliance with the AML/CFT/CPF laws of Trinidad and Tobago. Failure to ensure compliance by the Registrant with the requirements of the AML/CFT/CPF laws may result in significant penalties for Directors and the Registrant. This includes information and analysis of transactions and activities which appear unusual (if such analysis was done). Similarly, branches and subsidiaries should receive such information from these group level functions when relevant and appropriate for risk management;

b. Subsidiaries and branches of Registrants, including those domiciled outside of Trinidad and Tobago are expected to, at a minimum, comply with the requirements of Trinidad and Tobago's AML/CFT/CPF laws;

c. Where some of a Registrant's operational functions are outsourced, the Registrant retains full responsibility for compliance with the AML/CFT/CPF laws of Trinidad and Tobago; and

d. AML/CFT/CPF Programmes must include adequate safeguards on the confidentiality and use of information exchanged, including the prevention of tipping-off.

7.8 Directors must therefore demonstrate their commitment to an effective AML/CFT/CPF Programme, by:

a. Understanding the statutory duties placed upon them, their staff and the entity itself;

b. Approving AML/CFT/CPF policies and procedures that are appropriate for the risks faced by the Registrant. Evidence of consideration and approval of these policies must be reflected in the Board Minutes;

c. Appointing an individual within the organisation to ensure that the financial institution's AML/CFT/CPF procedures are being managed effectively; and

d. Seeking assurance that the financial institution complies with its statutory responsibilities as it relates to AML/CFT/CPF. This includes reviewing the reports from compliance

reviews on the operations and effectiveness of compliance systems. See Guidelines 8.42-8.53 Internal and External Audit.

7.9 Senior management is responsible for development of sound risk management programmes and keeping Directors adequately informed about these programmes and their effectiveness. These programmes, which should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments, must be formally documented and, at a minimum, irrespective of whether the Registrant receives funds from third parties or not, must provide for:

a. The development of internal policies, procedures and controls for inter alia:
    i. The opening of customer accounts and verification of customer identity;
    ii. Establishing business relations with third parties (including custodians, fund managers, correspondent banks, business introducers);
    iii. Determining business relationships that the financial institution will not accept;
    iv. The timely detection of unusual and suspicious transactions, and reporting to the FIUTT;
    v. Internal reporting; and
    vi. Record retention.
b. The recruitment of suitable staff, appropriate to the nature and size of the business, to conduct identification and research of unusual transactions, as well as the reporting of suspicious activities;
c. An ongoing training programme designed to ensure adherence by employees to the legal and internal procedures, and familiarity with the dangers they and the business entity face and on how their job responsibilities can encounter specified ML, TF, and PF risks;
d. Designation of a manager or official employed at managerial level as the Compliance Officer who has the appropriate level of authority, seniority and independence to coordinate and monitor the compliance program, receive internal reports and issue suspicious transaction reports to the FIUTT;
e. Establishment of information management /reporting systems to facilitate aggregate and group-wide monitoring;
f. An effective independent risk-based oversight function to test and evaluate the compliance program; and
g. Screening procedures for hiring, and on-going systems to promote high ethical and professional standards to prevent the Registrant from being used for criminal activity.

7.10 Policies should be reviewed biannually and periodically reviewed for consistency where amendments have been made to the AML/CFT/CPF legislative framework, the business model, product and service offering. Special attention must be paid to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products.

7.11 In order to fulfil its oversight role effectively, the Board or responsible body should ensure that the reports and information that it receives adequately allows for the assessment of whether that AML/CFT/CPF framework is effective. Therefore, where there are shortcomings in the scope of information being submitted, the Board should request additional information or reporting which may allow for improvements in its oversight of the Registrant's AML/CFT/CPF framework.

7.12 Oversight of the AML/CFT/CPF framework may be demonstrated by, among other things:

a. Approval, and periodic review, of policies and/or procedures reasonably designed to ensure that the Registrant complies with the relevant legislation and guidelines;
b. Ensuring that AML/CFT/CPF deficiencies identified by regulators, external and internal auditors are appropriately documented, reported and tracked through to remediation;
c. Receipt of periodic reporting on ML/TF/PF risks and the Registrant's compliance with the AML/CFT/CPF legislative framework and policies and/or procedures; and
d. Ensuring that the designated Compliance Officer is of the highest levels of integrity and competence.

Risk-Based Approach – Institutional Risk Assessments

7.13 Recommendation 1 of FATF as well as the POCA and the FORs require Financial Institutions to identify and assess their ML, TF and PF risks (for customers, countries, or geographic areas; and products; services, transactions or delivery channels). These risk assessments should be documented in order to demonstrate the basis, keep the assessments up to date and have in place appropriate channels and mechanisms to provide the risk assessment information to Supervisory Authorities and CAs with the results of the risk assessment. Some of the key characteristics of the securities sector which make it more vulnerable to ML/TF/PF abuse are set out at **Appendix 1** of the Guidelines. The nature of

the securities sector means that the risks encountered by the Registrants may differ from those encountered by other financial institutions operating in financial sectors external to the securities sector. Therefore, Registrants are required to utilize a risk-based approach in the performance of all their AML/CFT/CPF responsibilities and must implement measures that are commensurate with their assessed risks. Prior to conducting risk assessments, Registrants should familiarize themselves with the sector's vulnerabilities. To execute an ML/TF/PF risk assessment, the Registrant should take appropriate steps to identify and assess the ML/TF/PF risks related to customers, countries or geographic areas, products, services, transactions and delivery channels. Further, in keeping with the requirement of FATF's Recommendation 15, FIs are required to identify and assess ML/TF/PF risks that may arise in relation to:

a. the development of new products and new business practices, including new delivery mechanisms, and
b. the use of new or developing technologies for both new and existing products.

7.14 Registrants are required to undertake these risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks. ML/TF/PF risks continue to evolve, therefore, requiring Registrants to ensure that these risks are continuously reviewed and updated.

7.15 The identification and assessment of ML/TF/PF risk is the first step in developing a robust AML/CFT/CPF programme. The risk assessment serves to assess the risk of ML/TF/PF a Registrant may reasonably expect to face during its business and the establishment of the risk profiles of its customers. The risk assessment also provides the basis for implementation of risk-based measures such as: Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) and Simplified Due Diligence (SDD) measures or other measures commensurate with the level of risk identified. Each Registrant must develop and implement an approved internal risk assessment and rating policy, which must include, at minimum:

a. **Risk Identification** - identify the ML/TF/PF risks which are specific to the Registrant itself and to its customers;
b. **Risk Analysis** - assess the risks identified and apply an appropriate risk rating;
c. **Risk Management** - monitor the risks identified in a manner which is proportionate to the risk rating; and

d. **Risk Monitoring and Review** - manage the risks identified with a view to mitigating such risks.

Risk Identification

7.16 Registrants must identify, assess and understand risks in terms of country, geographic location, customers, products, services, transactions and delivery channels. Based on the nature of the Registrant's business, additional categories may be considered. Registrants should determine the likelihood that any category may be misused as well as the impact of such actions.

7.17 Country - Factors a Registrant may consider in assigning risk scores includes the results of National Risk Assessments (NRA), Sector Risk Assessments, CFATF Mutual Evaluation Reports as well as FATF's publications on high risk and other monitored jurisdictions.

7.18 NRAs are conducted to identify, assess and understand ML/TF/PF threats and vulnerabilities faced by a jurisdiction. Identifying, assessing, and understanding ML/TF/PF risks is an essential part of the implementation and development of a national AML/CFT/CPF regime, which includes laws, regulations, enforcement and other measures to mitigate ML/TF/PF risks. The results of an NRA can provide useful information to Registrants to support the conduct of their own risk assessments. Within the NRA, sectoral assessments provide a detailed view of inherent vulnerabilities and control effectiveness of a nation's key sectors. The significance of the NRA report makes it a critical source of information contributing to a Registrant's institutional risk assessment. Information provided by the NRA can help Registrants identify and evaluate country-specific risks. In doing so, Registrants can determine how those risks might impact their business and what steps they can take to manage or mitigate those risks.

a. The primary objective for disseminating the NRA report is to apprise all stakeholders of the main sources and drivers of the ML/TF/PF risks in order to develop effective risk-based policies and actions and allocate the available resources in the most efficient way to mitigate the identified ML/TF/PF risks to the country.
b. Registrants should consider the findings of the NRA report that are relevant to their sector whilst conducting their institutional risk assessment, as areas determined by the

NRA report that represent a high ML risk cannot be over-ruled in the risk assessment process of a Registrant.

c. Nature, Size and Complexity – The size and complexity of the business play an important role in how susceptible it is for ML/TF/PF. For example, businesses that accept cash from customers are at greater risk for ML/TF/PF than those accepting cheques or bank transfers. A business that conducts complex transactions across international jurisdictions could offer greater opportunities to launderers than a purely domestic business. Registrants should consider the ability of their customers to use the business to allocate their funds across numerous products to avoid detection.
d. Using internal data, Registrants can identify their ML/TF/PF vulnerabilities in their business activities. For instance, the risk assessment will be flawed where Registrants identify a higher-risk product but may be oblivious to the number of customers who have been provided with these products, and where they are domiciled.

7.19 Geographic location – Identifying geographical locations that may pose a higher risk is a core component of any inherent risk assessment. Registrants should seek to understand the risks associated with different geographical locations to evaluate the specific risks associated with doing business in or offering products / services in certain geographical locations. As such, the risk assessment must consider the risks associated with jurisdictions in which Registrants operate as well as the risks associated with jurisdictions in which customers of Registrants conduct business. Registrants should conduct an analysis to understand their geographic footprint and determine customers within each country. This analysis can be based on one or all the following:

a. domicile;
b. nationality and/or
c. incorporation.

The geographic risk can also result from the following:

a. Countries / areas identified as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them;
b. Countries identified as having significant levels of organised crime, corruption or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling;

c. Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations; and
d. Countries identified as having weak governance, law enforcement and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes and for which financial institutions should give special attention to business relationships and transactions.

7.20 When assessing the geographical location risk, Registrants should consider country reports from international organisations that identify countries that are subject to economic sanctions, those known to be supporting international terrorism and those with deficiencies in combatting ML/TF/PF, such as a list of high risk and other monitored jurisdictions published by:

a. FATF list of high-risk and jurisdictions under increased monitoring;
b. FATF and CFATF Mutual Evaluation Reports;
c. European Union AML and tax blacklists;
d. United Nations Office on Drugs and Crime ("UNODC") reports;
e. Transparency International Corruption Perception Index;
f. Organisation for Economic Cooperation and Development's ("OECD") country risk classification; and
g. U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") sanctions list including the Specially Designated Nationals and Blocked Persons List ("SDN").

7.21 Customer / Investor - Certain categories of customers pose a higher ML/TF/PF risk than others, especially when combined with higher risk products, services or geographic locations. Registrants therefore must understand the risks associated with their customers. When assessing a customer / investor risk, it is essential that Registrants establish criteria for identifying high-risk customers. The following factors can be used to establish the customer's risk:

a. Customer type/profession: Certain individuals may present elevated risk;
b. Country of domicile - Customer residing in jurisdictions that are uncooperative in providing Beneficial Ownership (BO) information, or whose primary source of income originates from high-risk jurisdictions (regardless of income source);

c. Ownership structure - Customer who has a non-transparent ownership structure and who is a legal entity whose ownership structure is unduly complex;
d. Industry / Nature of business activities: Businesses operating in high-risk sectors;
e. Past activities - Unusual or sudden changes in transaction behaviour that deviate from regular patterns are critical indicators;
f. Political / Government role- Individuals holding or associated with politically exposed positions;
g. Source of funds;
h. Type of assets;
i. Frequent or unexplained transfers to various institutions, movements of funds between different jurisdictions;
j. Product usage; association with high net worth individuals;
k. Transactional activity (size, volume, type, unusual);
l. Customer who is sanctioned by the relevant national competent authority for non-compliance with the applicable AML/CFT/CPF regime and is not engaging in remediation to improve its compliance;
m. Registrants should consider that certain categories of customers pose a perceived higher risk, such as, Politically Exposed Persons ("PEPs") who are generally considered as a higher risk of ML/TF when operating in countries with higher levels of bribery and corruption.

7.22 Transaction, Products and/or services – Due to the nature of certain products and services they are vulnerable to ML/TF/PF risk. As such, during the risk assessment process, it is the responsibility of Registrants to identify and assess the inherent ML/TF/PF risks associated with the products and services they offer. The identification should include the existing products and services and those under development or to be launched, such as future product offerings. This is necessary to assist Registrants to ascertain whether the existing AML/CFT controls will be adequate to manage the risks arising out of the new product or if any additional controls are necessary. The following broad categories should be considered when assessing product and services risk:

a. The level of transparency, or opaqueness of the product, service or transaction, that may inherently favour anonymity or obscure information about underlying customer transactions;

b. The complexity of the product, service or transaction with unusual complexity or structure and with no obvious economic purpose;
c. The value or size of the product, service or transaction;
d. Ease of convertibility of the product to cash, and change of ownership and products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction;
e. Length of time before the investment product matures:
f. Percentage of foreign ownership of the product, internationally traded products, etc.;
g. The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions;
h. Use of new technologies or payment methods not used in the normal course of business by the securities provider;
i. Products that have been particularly subject to fraud and marker abuse, such as low-priced securities;
j. Transactions that are one-off and non-face to face, prepaid card transactions, as well as transactions arising from the use of new technology, etc.

7.23 Delivery channels - Certain delivery channels may increase ML/TF/PF risk as they contribute to challenges when it comes to understanding the identity and activities of customers. Therefore, Registrants must consider the risks associated with the way the products and services are delivered to the customers. Certain delivery channels such as non-face-to-face, may pose a higher ML/TF/PF risk as they increase the challenge of verifying the customer's identity and activities. The following broad categories should be considered when assessing the risk of delivery channels:

a. The extent to which the business relationship is conducted on a non-face-to-face basis;
b. Use of introducers or intermediaries and the nature of their relationship with the Registrant; and
c. Any other third-party involvement and the nature of this involvement such as the use of on-line services, wire transfer services, transfers through intermediaries.

d. Products or services distributed directly through online delivery channels should identify and assess the ML/TF/PF risks that may arise in relation to distributing its products or services using this business model;
e. The risk assessment process for online delivery risk should be performed when Registrants develop new products and new business practices;
f. Use of intermediaries
g. Suspicion of criminal activities, particularly financial crimes or association with criminal associates[3];
h. Located in a higher risk country or in a country with a weak AML/CFT regime;
i. Serving high-risk customers without appropriate risk mitigating measures;
j. A history of non-compliance with laws or regulations or that have been the subject of relevant negative attention from credible media or law enforcement agencies; and
k. that have weak AML/CFT controls or operate sub-standard compliance programmes, i.e. programs that do not effectively manage compliance with internal policies and/or external regulation or the quality of whose compliance programmes cannot be confirmed.

Other Factors

7.24 The NRA and sector risk assessments are useful sources of information when identifying how Registrants could be used for ML/TF/PF. Registrants should also consider emerging trends that are indicated by the TTSEC and/or FIUTT in their guidance when identifying risks in its business. Information on current ML/TF/PF methods available on the FATF website / other international standard setting bodies can be relied upon when assessing the risk its business could be reasonably expected to face.

7.25 Given the evolving nature of AML/CFT/CPF expectations and requirements, Registrants should assess whether they have identified new or emerging risks that substantially alter their risk profile. Registrants should enhance their risk assessment when they observe any

[3] The risk of criminal activity through delivery channels involves the possibility that a company's products or services could be used by criminals for illicit purposes, such as money laundering or terrorist financing. This risk can manifest as suspicious transactions like large cash deposits, unusual asset purchases, or the use of third parties for transfers, and is heightened by certain customer types, high-risk business sectors, and complex ownership structures.

changes in the ML/TF/PF risks of their business to determine the institution's risk profile and appropriate level of mitigation to be applied.

Risk Analysis

7.26 Registrants must assess all relevant risk categories identified above as well as assess the ML/TF/PF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products and assign ratings based on the likelihood and impact that the risk posed to business operations. Registrants may utilise a risk matrix as a method of assessing risk to identify inherent risk factors that are low risk, those that carry medium but acceptable risk and those that carry a high or unacceptable risk of ML/TF/PF. An overall risk rating is then developed and the appropriate level of mitigation to be applied is determined. The risk matrix is not static; it changes as the circumstances of the Registrants change.

7.27 Registrants, in classifying the risk after considering its specificities, may also define additional levels of ML/TF/PF risk. A risk analysis will assist Registrants to recognise that ML/TF/PF risks may vary across customers, products/services, delivery channels and geographic location and thereby focus their efforts on high-risk areas in their business.

7.28 Registrants must ensure that the risk identification and analysis is appropriately documented to demonstrate its basis and provide the risk assessment information to the TTSEC, upon request. Where Registrants use automated IT systems to allocate overall risk scores to inherent risk indicators and do not develop these in-house but purchase them from an external provider, Registrants should understand how the system works and how it combines risk factors to achieve an overall risk score. Registrants must always be able to satisfy themselves that the scores allocated reflect the Registrants' understanding of ML/TF/PF risk and should be able to demonstrate this to the TTSEC.

7.29 Registrants should consider the following non-exhaustive risk criteria when assessing and determining the risk rating and risk profile of clients:

a. Whether or not the individual is a PEP;
b. The geographical origin of the client;

c. The geographical sphere of the client's business activities including the location of the counterparties with which the client conducts transactions and does business, and whether the client is otherwise connected with high risk jurisdictions;
d. The nature, size and complexity of the client's business;
e. The nature and frequency of activity, in relation to the knowledge the Registrant has about the client;
f. The type, value and complexity of the security;
g. The unwillingness of the client to cooperate with the Registrant's CDD process for no reason;
h. The undue complexity of a corporate client's ownership structure;
i. If the business is a non-profit organisation;
j. Occasional and one-off transactions;
k. If the business is cash-intensive;
l. The existence of any delegated form of authority such as but not exclusive to a power of attorney;
m. The product or service utilized by the client;
n. Situations where there is difficulty in determining the source of wealth and/or source of funds, or where the audit trail has been broken or layered;
o. Whether the account/business relationship is dormant; and
p. Any other information that raises suspicion of the client being connected to ML or TF activities.

Risk Management

7.30 Internal controls are procedures or policies put in place by Registrants to prevent their services from being used to facilitate ML/TF/PF or to ensure that potential risks are promptly identified. Internal controls are also used to maintain compliance with regulations governing the activities of Registrants. After Registrants have identified and assessed risks, they should proceed with assessing the quality of the existing AML/CFT controls to determine the operating effectiveness of the controls in managing the identified risks. A review of internal controls and test for effectiveness should be done on an on-going basis to assess whether any change in the inherent risk of Registrants or residual risk necessitates enhancement of such controls. Audits [see Guidelines 8.40-8.53] should also be considered to determine the effectiveness of the AML/CFT controls. The assessment of inherent risk

and internal controls along with effective implementation of mitigating factors will improve the residual risk of Registrants.

7.31 Registrants are required to have policies, procedures, systems and controls in place to:

a. Monitor the risks identified in its risk assessment within a time and manner that is proportionate to the risk level assigned; and
b. Manage the risks identified with a view to mitigation of those risks.

7.32 These policies, controls and procedures should also be monitored and reviewed periodically and updated in a timely manner so that they can be enhanced, if necessary, in light of changing or emerging risks. The frequency of the review should be documented in the AML/CFT/CPF compliance programme.

7.33 These policies, controls and procedures must be approved by the Board of Directors or senior management of the Registrant and must be consistent with local AML/CFT/CPF Legislative Framework and the Guidelines. The risk-based policy should also contain procedures for:

a. Clear documentation of all AML/CFT/CPF risk assessments.
b. Clear documentation of the risk assessment methodology, including the rationale behind the risk rating assigned and approved by the Board of Directors of Registrants. The risk assessment should describe, the methodology employed and any measures undertaken by Registrants to manage the identified risks and should be consolidated within a comprehensive report and communicated to the Board of Directors and senior management in a timely, complete and accurate manner to assist them in making informed decisions and ensuring that the resources, expertise and technology of Registrants are aligned and effectively engaged in mitigating the identified risks. Registrants shall submit the results of the updated risk assessment to the Authority and law enforcement agencies upon request, as provided under Regulation 7(2)(c) of the FORs.
c. Ensuring that changes to the risk ratings of clients are documented, the reasons for the changes clearly outlined and approval of any change to risk ratings are obtained;
d. Application of SDD, CDD and/or EDD measures in accordance with the assigned risks;
e. Recording reasons for not complying with the organisations risk mitigation policies, procedures and controls contained in the Risk-Based Policy;

f. Review of the high-risk clients' risk assessment more frequently than medium and low risks clients[4]. Frequency of reassessment of clients should be commensurate with the risks identified. Where necessary, a determination regarding the continuity of the business relationship should be assessed by senior management. All decisions regarding the discontinuation of business relationships with high-risk clients should be approved by senior management and documented.

7.34 When deciding to discontinue a business relationship, the Registrant should consider whether a Suspicious Activity Report (SAR) should be made to the FIUTT and whether terminating the relationship would tip off the client.

7.35 Registrants must provide appropriate tools / software systems, frameworks and sufficient training for staff to effectively implement, identify, assess, and manage risks.

Ongoing Monitoring and Review and ML/TF Risks

7.36 Regulation 37 of the Financial Obligations Regulations 2010 (as amended) ("FOR") requires a financial institution to monitor and conduct ongoing due diligence on existing customers on the basis of materiality and risk, taking into account the timing and adequacy of customer due diligence ("CDD") information previously collected.

7.37 Ongoing monitoring of customer relationships is a critical component of an effective AML/CFT/CPF[5] risk management programme which:

a) serves to maintain a proper understanding of a customer's business activities, and ensures that there is consistency between expected and actual activity/transactions;

b) provides inputs for ongoing assessment of ML/TF/PF risks; and

c) assists with detecting and reviewing unusual or suspicious activities and transactions.

[4] High-risk clients should be reviewed at least **annually**. The exact frequency depends on the client's risk profile and your company's risk-based policy, but a high-risk classification typically requires more frequent and intensive reviews than for medium- or low-risk clients. Medium risks may be reviewed every three years whilst low risk clients, every three to five years.

[5] AML/CFT/CPF means Anti-Money Laundering/Combating the Financing of Terrorism/Countering Proliferation Financing. Therefore, ML/FT/PF shall be construed accordingly.

7.38 Ongoing monitoring should be conducted on all customer relationships. However, in line with a risk-based approach, financial institutions have the flexibility to adjust the extent and depth of monitoring based on the customer's ML/TF/PF risk profile. Policies and procedures for ongoing monitoring must demonstrate that CDD measures and monitoring processes are appropriate and risk-based.

Maintaining relevant and up-to-date CDD data, documents and information is fundamental to conducting ongoing monitoring effectively, and for identifying changes to the customer's risk profile. Importantly, identifying variances between expected and actual activity/transactions depends on obtaining information on the nature and intended purpose of the business relationship at the outset of the relationship, to enable monitoring, detection and analysis of subsequent unusual and suspicious activity/transactions. The relevant CDD information that should be collected at the outset of a customer relationship is codified in Regulations 15, 16 and 17 of the FOR and additional guidance is provided in Part 3 of the AML/CFT Guideline. CDD information to be collected may include where applicable:

a) the customer's/beneficial owner's business activities/occupation/employment;

b) the geographical location of the customer's/beneficial owner's physical residence, business operations and assets;

c) the ownership and control structure where the customer/beneficial owner of the customer is a legal person or legal arrangement;

d) the types of financial products/services the customer may utilize;

e) the expected type, volume, frequency and value of activity that would be conducted utilizing the financial institution's products and services;

f) the beneficial owners, controllers, directors and signatories[6]; and

g) the customer's counterparties, related third parties and the nature of their relationships with the customer/ beneficial owner.

[6] Examples of identifying information that should be collected include the full legal name, nationality(ies), date and place of birth, residential address, national identification number and document type.

Conducting Periodic Reviews of Customer Relationships

7.39 Guideline 7.38 did not specify a period for re-assessment of lower risk customers' ML/TF risk profile. However, the TTSEC suggests that the frequency of periodic reviews for customers other than high-risk customers, may be based on trigger events or, in the absence of a trigger event, at a minimum, the review should be undertaken every three (3) years for standard or medium risk customers, and every five (5) years for low-risk customers.

7.40 Registrants must ensure they have implemented effective and appropriate policies and procedures for event-driven and scheduled reviews of customer relationships. Employees must be provided with specific training and procedures on how to undertake periodic reviews.

7.41 Policies and procedures for conducting periodic due diligence reviews should, at a minimum, address the following:

a) proactive utilization of customer contact points as an opportunity to update CDD information;

b) risk-based procedures for ensuring that beneficial ownership information for legal persons and legal arrangements is accurate and updated within a reasonable period following any change;

c) clearly articulated due diligence review procedures to be undertaken for low-risk customers to be distinguished from the due diligence applicable for standard, medium or high risk customers. This should include the extent and type of CDD data, documents and information that should be updated for each customer category on a riskbasis, including:

- when identity information, source of funds or wealth should be verified;
- when additional investigations or requests for information should be made regarding a customer's business or the reasons for a transaction; and
- how much transactional history, types of transactions should be reviewed;

d) the circumstances that would trigger a review, including:

- changes in legislation or internal policies;
- material changes in legal or beneficial ownership of a legal person or arrangement, its directors, or authorized signatories, which should prompt an update to the due diligence information/documents for the relevant natural persons;
- changes in other relevant data, such as name, registered address, business operations of a legal person or arrangement;

- business expansion through mergers and acquisitions or into new markets/customer segments;
- requests for new financial products or services;
- legal proceedings against a customer or beneficial owner;
- discovery of materially adverse information such as reports of allegations or investigations of fraud,

corruption or other crimes;

- qualified opinion from an independent auditor on the financial statements of a legal person;
- transaction activity that deviates from established norms;
- adverse information received from a competent authority;

e) an assessment of whether the account activity is consistent with the purpose and anticipated account activity established at on-boarding, and whether the account activity is consistent with the customer's established source of funds/business operations and where applicable, their source of wealth;

f) screening of the customer, directors, authorized signatories and the legal and beneficial owners against designated sanctions lists and to identify new PEP relationships;

g) conducting open source searches to identify adverse indicators that may elevate the risk profile;

h) reassessment and if applicable, re-categorization of the customer's risk rating upon material updates to CDD information, obtained either through a trigger event or scheduled review;

i) obtaining and maintaining evidence of senior management approval for changes to the customer risk rating and for the continuation of business relationships with PEPs and high risk customers;

j) the action required when appropriate CDD documentation or information is not obtained during the review, including the steps and timelines that may be taken to obtain such documentation or information, and actions to be taken to mitigate ML/TF/PF risk when CDD information cannot be obtained after reasonable efforts have been made to update the information;

k) documentation of the findings and outcomes of the periodic reviews, including documentation of the rationale to maintain or change the customer's risk rating;

l) determination of whether account activity, adverse media alerts or outcomes of the review represent unusual or suspicious activity requiring further investigation; enhanced monitoring or termination of the customer relationship; or reporting to the FIUTT; and

m) independent audit reviews of the quality and effectiveness of CDD reviews and updates.

8. PART 2: Compliance Programme

8.1 An AML/CFT/CPF Compliance Programme sets out the internal policies, procedures and controls necessary to detect ML/TF/PF and to manage and mitigate the risk of it occurring. For the purposes of these Guidelines:

a. Policies set out expected behaviour and required standards in business as they play a crucial role in the entity's governance, risk management, and ensuring that activities are conducted in a manner that aligns with its values and objectives;
b. Procedures are detailed step-by-step methods outlining how specific tasks or activities should be executed within an organisation. Procedures offer a more granular level of instruction on how to perform particular functions or processes and are developed to ensure consistency, efficiency, and compliance with established standards; and
c. Controls are tools that management use to ensure the business complies with policies and procedures.

8.2 The policies, procedures and controls that are implemented must be adequate and effective and must be sufficiently robust to reasonably address the risks outlined in a Registrant's risk assessment. For example, if a Registrant rated a particular type of customer as "high-risk" in the risk assessment, the AML/CFT/CPF programme should reflect this risk rating with adequate and effective policies, procedures and controls. This should include a policy to conduct enhanced due diligence on such customers, the procedures for doing so and the necessary controls to ensure that the appropriate treatment follows.

8.3 Each Registrant must develop and implement a written AML/CFT/CPF Compliance Programme, approved by the Registrant's Board of Directors and designed to ensure compliance with the AML/CFT/CPF suite of legislation.

8.4 A Registrant who is part of a financial group must ensure that its group-wide AML/CFT/CPF compliance programme is applicable and appropriate to all subsidiaries and branches of the financial group. Specifically, the implementation of the group AML/CFT/CPF compliance programme should be tailored to the Registrant's particular business operations and risks.

8.5 Regulation 7(4) of the FORs identifies measures, to which Registrants are required to adhere, for the application of Group-wide compliance programmes including:

a. Policies and procedures for information sharing within the group for the purposes of CDD and ML/TF/PF risk management;
b. Provision, at group level compliance, audit and AML/CFT/CPF functions of client, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and
c. Adequate safeguards on confidentiality and use of information exchanged including safeguards to prevent tipping-off.

8.6 An AML/CFT/CPF Compliance Programme referred to in Regulation 7(1) of the FORs must be based on the Registrant's risk assessment and must include—

a. a system of policy, procedure and controls to ensure ongoing compliance;
b. customer identification and verification and other customer due diligence measures;
c. internal and external independent testing for compliance;
d. the identification and internal reporting of suspicious transactions and activities; and
e. appointment of a compliance officer who will be responsible for continual compliance with the AML/CFT/CPF legislative framework; and
f. Retention of records and other information.

8.7 An AML/CFT/CPF Compliance Programme must contain explicit references to any supplemental policies and procedures which may have been incorporated into the AML/CFT/PF framework.

8.8 A Registrant's written AML/CFT/CPF Compliance Programme must be made available to all new and existing employees and be easily accessible for reference and training purposes.

8.9 The Registrant should periodically monitor and review its AML/CFT/CPF Compliance Programme and must be promptly updated when there are amendments to the legislation and its risk assessment.

Designation of Compliance Officer and Alternative Compliance Officer

8.10 A Registrant must designate a CO and ACO employed at a managerial level. In this regard, Registrants should examine its organisational structure and ensure placement of the CO and ACO is at the requisite level in the organisation.

8.11 A Registrant who is part of a financial group may for the purpose of securing compliance with the AML/CFT/CPF laws and regulations, designate a CO employed at the managerial level within the financial group who is also the CO for another financial institution within the financial group.

8.12 Where a Registrant employs five persons or fewer, the employee holding the most senior position must be designated as the CO. In the case of a Registrant who is an individual who does not employ or act in association with any other person, that Registrant will assume the duties of the CO.

8.13 To ensure that the duties of a CO are adequately discharged during periods of the CO's absence, the Registrant must appoint a senior employee as an ACO in keeping with Regulation 8 of the FORs to fulfil the functions of the CO as defined by Regulation 4 of the FORs.

8.14 The ACO must have the same responsibilities as the CO and all requirements and responsibilities stipulated for the CO must apply equally to the ACO.

8.15 A Registrant who is an individual and has no one in his employ does not need to appoint an ACO.

8.16 Registrants must seek approval of TTSEC for appointment of its designated CO and the ACO.

8.17 Applications for approval of COs and ACOs should be made to TTSEC in the manner as directed by TTSEC and should be accompanied by all requested documents.

8.18 Where a Registrant is also registered with the CBTT, the Registrant must submit applications for approval of a CO simultaneously to each Supervisory Authority. The application to each Supervisory Authority should indicate that an application was also submitted to the other Supervisory Authority. The Supervisory Authorities will consult with each other on the suitability of the applicant and responses will be conveyed by each SA to its respective licensee or registrant.

8.19 TTSEC's application process for approval of COs and ACOs can be found on TTSEC's website: https://www.ttsec.org.tt/industry/aml-cft-cpf/reporting-application-forms-questionnaires/.

8.20 The identities of the CO and ACO must be treated with strictest of confidentiality by the Registrant and all members of staff.

8.21 A Registrant should apply to the TTSEC for approval of the CO and ACO, within seven (7) days of selection/appointment of a person to undertake the position of CO or ACO.

8.22 Registrants should ensure that COs and ACOs receive appropriate training to enable them to detect potential money laundering and terrorist financing activities and perform all other duties as set out in the Guidelines and the FORs.

Functions of the Compliance Officer

8.23 The CO has overall responsibility for implementation of the Registrant's AML/CFT/CPF compliance programme. At a minimum, the CO must perform the functions and duties as prescribed in Regulation 4(1) of the FORs and among other things should:

a. Have oversight of the AML/CFT/CPF controls in all relevant business areas for purposes of establishing a reasonable threshold level and consistent application of controls across all relevant business areas to maintain a cohesive and effective approach to AML/CFT/CPF compliance throughout the Registrant's business;

b. Keep the written AML/CFT/CPF compliance programme, procedures and controls updated relative to the Registrant's identified inherent risks with consideration given to local and international developments in ML/TF/PF and approved by the Board of Directors;
c. Ensure regular risk assessments of the inherent ML/TF/PF risks including timely assessments of new products, services, delivery mechanisms, use of new or developing technologies for both new and existing products and business acquisition initiatives to identify potential ML/TF/PF risks and develop appropriate control mechanisms, are conducted;
d. Ensure systems resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the Registrant's business;
e. Ensure that all new and existing employees, senior management and the Board of Directors participate in ongoing AML/CFT/CPF training programmes, which are up-to-date and relevant to the Registrant's business;
f. Ensure that systems and other processes that generate information used in reports to senior management are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information;
g. Report relevant information to the Board of Directors and/or senior management regarding the adequacy of the AML/CFT/CPF framework or any associated issues; and
h. Ensure any changes to the AML/CFT/CPF compliance programme are disseminated to all employees and assist departments in implementation of the AML/CFT/CPF compliance programme.

8.24 The duties and responsibilities performed by the CO should be documented in the COs Job Description.

8.25 For consistency and to ensure ongoing attention to the compliance regime, the appointed CO may delegate certain duties to other employees. However, where such delegation occurs, the CO must retain responsibility and accountability for the AML/CFT/CPF Compliance Programme. The CO must have:

a. Unfettered access to, and direct communications with Senior Management and the Board of Directors; and

b. Timely and uninhibited access to client identification, transaction records and other relevant information throughout the organisation.

Know Your Employee

8.26 A Registrant must undertake appropriate due diligence on prospective and existing staff members. The extent of the screening should be determined by the level of responsibilities and risks inherent to the functions / positions of the existing or prospective employee.

8.27 The due diligence measures should include but are not limited to the following activities:

a. verification of identity and nationality;
b. verifying employment history, references, authenticity of academic qualifications; and
c. checking criminal record of the staff member/police certificate of character.

8.28 These screening requirements are in addition to the pre-employment measures Registrants would normally undertake to ensure that employees are fit and proper to hold the desired position.

8.29 A Registrant should ensure all employee files are kept current and accurate at all times. Employee records should include the names, addresses, position titles and other official information pertaining to staff members appointed or recruited by them. Records of former employees should be kept for a period of up to six (6) years after termination of employment. All records should be made available to the TTSEC upon request.

8.30 In addition to a robust recruitment policy, Registrants should implement ongoing monitoring of all employees to ensure they continue to meet the Registrant's standards of integrity and competence.

8.31 The Registrant's written policies, procedures and onboarding documents should include a code of ethics and an AML/CFT/CPF compliance programme, which must be attested to by all employees. These documents serve to guide all employees in the conduct of their duties and should be updated periodically.

8.32 AML/CFT/CPF policies and procedures should be applied consistently and at all levels of staff with disciplinary action being taken for failing to follow established procedures.

Education and Training of Employees

8.33 Registrants should establish and maintain a record of ongoing AML/CFT/CPF training programs for Directors, Senior Management and staff at all levels, both new and existing.

8.34 Training should be held at least once annually.

8.35 Records should be kept of the training course content provided as well as training attendance logs indicating, at a minimum, employee name and dates of attendance and/or completion of training.

8.36 The Registrant's training plan should, at a minimum, adequately address the Registrant's obligations under the Guidelines, all relevant legislation and any other written law by which the recommendations of the FATF are implemented.

8.37 The Registrant's training should enable its employees at all levels of the financial institution to:

a. identify the risks associated with ML/TF/PF, understand their ML/TF/PF risk exposure specific to their job function and understand how the institution might be used for ML/TF/PF;
b. be aware of techniques and trends utilized in ML/TF/PF;
c. be aware of the legal consequences for non-compliance with the Guidelines and related legislation;
d. be aware of processes for detecting ML/TF/PF transactions, and for reporting suspicious transactions and activities to their CO or ACO;
e. be aware of the identity, roles and responsibilities of the CO as well as the ACO to whom they should report unusual or suspicious transactions and activities.

8.38 New employees should undergo an orientation in AML/CFT/CPF generally and specific to their role in the Registrant's business within three months of employment.

A copy of the Registrant's approved AML/CFT compliance programme as well as all supplemental policies and procedures should be provided to new employees on assumption of duties and attestation that same was read and understood.

Conduct of Independent Testing

8.39 Regulation 10(2) of the FORs requires the Registrant to annually undertake, on a risk sensitive basis, an independent review of its compliance programme. For the purpose of this Regulation, the independent review means audits performed by the internal audit function. The scope of the review shall be at the discretion of the auditor on a risk sensitive basis, and shall include testing of customer files and transactions. The Registrant must make this available to the TTSEC upon request.

8.40 Regulation 10(3) of the FORs requires the Registrant to, on a risk sensitive basis, also conduct, at a minimum of every three years, or at such frequency as the TTSEC may specify, a comprehensive and independent review of:

a. its compliance with the relevant legislation and guidelines; and
b. the reliability, integrity and completeness of the design and effectiveness of:
    i. the compliance risk management function; and
    ii. the internal controls framework,

and submit reports and recommendations to the Board of Directors of the financial institution upon completion of the review and to the TTSEC upon request and within such timeframe as specified.

8.41 The comprehensive audit as outlined in 8.41 requires the Registrant to conduct a comprehensive audit at least every three years and the audit must be based on the scope as outlined in 8.41 (a) and (b).

8.42 It is the Registrants' responsibility to ensure that the independent auditor or competent professional for the purpose of Regulation 10 is specifically trained to undertake their functions, having appropriate AML/CFT training and experience in respect of ML and TF risk and an appropriate level of knowledge of the regulatory requirements and guidelines. The Registrant shall apply the following measures when selecting an auditor or competent professional to fulfil their obligation under Regulations 10 (4) FORs:

- **Expertise and Qualifications**: Ensure the candidate possesses expertise in AML/CFT/CPF compliance, supported by relevant qualifications and certifications in law, finance, or related fields.
- **Knowledge of Regulations**: the candidate has a thorough understanding of AML/CFT/CPF laws, regulations, and international standards, such as those set by the FATF.
- **Experience**: Ensure the candidate has prior experience conducting AML/CFT/ CPF audits and possess knowledge of best practices within the securities sector.
- **Integrity and Competence**: Prioritize candidates with a reputation for integrity, reliability, and high ethical standards. Conduct thorough background checks and seek references to verify their reputation.
- **Independence**: Ensure that the candidate maintains independence and impartiality throughout the testing process to provide unbiased and objective results.

8.43 The internal audit department / internal auditor must conduct an independent evaluation of the compliance programme to evaluate its adequacy, completeness and effectiveness on a risk basis. The review process must identify and note weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions.

8.44 The TTSEC acknowledges that the establishment of an internal audit department might pose challenges for smaller Registrants, and as such where this is not feasible, a Registrant may outsource the operational aspects of the internal audit function to a person or firm that is not involved in the auditing or accounting functions of the Registrant.

8.45 Auditors are required to document the audit scope, procedures conducted, transaction testing outcomes, and findings of the review. All audit documentation must be accessible for TTSEC's review upon request. Any breaches, policy or procedure exceptions, or other shortcomings identified during the audit should be recorded in an audit report and promptly communicated to senior management and the Board or a designated committee. Senior management should provide guidance on corrective measures to rectify deficiencies and establish a timeline for their implementation. The Board or designated committee, along with the audit, should monitor audit deficiencies and ensure that corrective actions are promptly executed.

8.46 The Internal Auditor must ensure that the level of transaction testing conducted is suitable to the client's risk profile.

8.47 The internal audit may include, inter alia:

a. A review of the Registrant's risk assessment and rating policy for reasonableness given its risk profile as set out in the Guidelines;
b. Determining the adequacy of the Registrant's ML/TF/PF risk assessment framework and application of a risk-based approach in the design of its AML/CFT/CPF policies, procedures and controls;
c. Appropriate risk-based testing of client files and transactions to verify adherence to the AML/CFT/CPF recordkeeping (including initial CDD and ongoing CDD information) and reporting requirements;
d. An evaluation of management's efforts to resolve breaches and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable;
e. A review of employee training for effectiveness, completeness and frequency and the extent of employees' and officers' (including senior management's) compliance with established AML/CFT/CPF policies and procedures;
f. A review of the effectiveness of the suspicious activity/transaction monitoring systems (manual, automated, or a combination) used for AML/CFT compliance including a review of the criteria and processes for identifying and reporting suspicious transactions;
g. An assessment of the overall process for identifying and reporting suspicious activity, including a review of 'not filed' (closed, not suspicious) internal suspicious transactions/activity reports to determine the adequacy, completeness and effectiveness of the adjudication process.

8.48 The internal audit review should include interviews with key employees, such as staff of the compliance unit, customer-facing staff and their supervisors to determine their knowledge of the AML/CFT/CPF legislative requirements and the Registrant's policies and procedures.

8.49 The internal audit review process should identify weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions, ensuring that recommendations made by the external auditor and the TTSEC have been satisfactorily addressed.

8.50 In addition to being specifically trained to conduct an AML/CFT/CPF internal audit, the internal auditor must be a person sufficiently independent of the development of the compliance program to ensure objectivity.

8.51 The internal auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of established AML/CFT/CPF measures and inadequacies in internal controls and procedures including recommended corrective measures.

Audit Finding Remediation Tracking System

8.52 To enhance accountability and ensure timely resolution of audit findings (both internal and external), Registrants should implement a robust tracking system for the remediation process. This tracking system should effectively monitor the progress, status, and resolution of identified audit issues and are made available to the TTSEC upon request. The purpose of this initiative is to promote transparency, facilitate communication, and allow for a third-party review. The tracking system should include, but is not limited to, the following elements:

a. *Identification and Logging*: Promptly log all audit findings in a centralized system, clearly documenting the nature of the issue, its severity, and the responsible party.
b. *Assignment of Responsibility*: Clearly assign responsibility for each finding to an accountable individual or team, ensuring clarity on who is responsible for remediation.
c. *Due Dates and Timelines*: Establish realistic and achievable due dates for remediation of each finding, reflecting the urgency and priority of the identified issues.
d. *Status Updates*: Regularly update the tracking system to reflect the current status of each finding, indicating whether it is in progress, resolved, or requires further attention.
e. *Documentation of Remediation Actions*: Record the actions taken to remediate each finding, providing sufficient detail of the corrective measures.
f. *Escalation Procedures*: Implement clear escalation procedures for findings that face challenges in resolution, ensuring timely communication to appropriate levels of management.

9. PART 3: CUSTOMER DUE DILIGENCE (CDD)

General CDD

9.1 CDD is a process that financial institutions and other regulated entities use to gather information about their customers/clients to assess and manage risks associated with financial transactions, ML/TF/PF, and other illicit activities. CDD aims at protecting the Registrant against customers/clients who may misuse the Registrant for the purpose of ML/TF/PF. CDD is a vital element within the broader framework of AML/CFT/CPF efforts. As mandated by FORs, CDD should be integral to every organization's risk management plan. Effectively implementing CDD measures is essential for mitigating the risk of ML/TF/PF, thus ensuring the overall integrity and security of financial systems. The key objectives of Customer Due Diligence include:

a. **Risk Assessment**: Understanding the level of risk associated with a customer, considering factors such as their business, transaction patterns, and geographic location.
b. **Identity Verification**: Verifying the identity of customers to ensure they are who they claim to be. This often involves collecting official documents like government-issued IDs, passports, or drivers permit.
c. **Understanding Business Relationships**: Examining the nature of the business relationship between the customer and the Registrant, including the purpose of the relationship and expected account activity.
d. **Monitoring Transactions**: Keen observation on customer transactions to identify any unusual or suspicious activities that may indicate money laundering or other financial crimes.
e. **Ongoing Due Diligence**: Continuously reassessing customer information and conducting periodic reviews, especially for high-risk customers or those involved in complex transactions.

9.2 As a basic prudential principle, Registrants should know the identity of the person they are transacting business with and the purpose of the transaction. A registrant shall conduct ongoing due diligence on a business relationship including ensuring that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories

of customers. (Refer to Guideline 9.50 for further guidance on Ongoing Due Diligence). CDD applies to both retail and institutional customers/clients.

9.3 Registrants are required to conduct customer due diligence, including verification of customer identity in circumstances which include, but are not limited to, the following:

a. Establishing a business relationship;
b. For one-off or occasional transactions of a value equivalent to TT$50,000 or more;
c. For two or more one-off transactions which together total a value equivalent to TT$50,000 or more and which appear to be linked;
d. For one-off wire transfers of a value equivalent to TT$6,000 or more;
e. For two or more one-off wire transfers which appear linked and which in total amount to a value equivalent to TT$6,000 or more;
f. If the Registrant has doubts about the veracity or adequacy of client identification data which was previously or otherwise obtained; and
g. Where there are reasonable grounds to suspect that the funds used may be linked to money laundering or terrorist financing, unless doing so would result in tipping-off. In such instances, the Registrant may forego CDD and must file a STR with the FIUTT.

9.4 Notwithstanding the thresholds established in law, Registrants may establish lower reporting thresholds that are commensurate with the size of transactions that are typically conducted at the Registrant.

9.5 Any client's transaction which falls within the parameters identified above at Guideline 9.3 must be accompanied by relevant documentation to substantiate the Source of Funds of each transaction. In addition to capturing the required substantiating documentation, Registrants may utilize a Source of Funds Declaration Form.

9.6 Documentation to substantiate the source of funds may be used to support a series of transactions undertaken by a client. The value represented by the documentation must be commensurate with the sum of the series of transactions and cannot be used to support transactions in excess of the initial supporting documentation kept on file. Where a bank statement (or financial statements for a business) is used as supporting documentation, the Registrant should, as part of ongoing due diligence, request an updated statement on a

periodic basis using a risk-based approach. The Registrant should have controls in place to trigger the need for new or additional documents to substantiate further transactions that exceed the initial source of funds.

9.7 Where a Registrant is unable to apply CDD measures, it shall

(a) not open an account or carry out a transaction for the customer;

(b) not establish a business relationship or carry out an occasional transaction with the customer;

(c) terminate any existing business relationship when the Registrant is unable to undertake ongoing monitoring with respect to the relationship; or

(d) undertake any further transactions of any nature until such time as it has been able to apply the customer due diligence measures

9.8 Where a Registrant takes any action in accordance with Guideline 9.7, Registrant shall consider whether a suspicious transaction report or suspicious activity report should be filed with the FIUTT.

9.9 Where at any time, a Registrant is in doubt about the veracity and adequacy of any information previously given by a customer, due diligence procedures shall be performed and where there are discrepancies in the information previously provided, the Registrant shall make every effort to obtain the correct information. Where the foregoing information cannot be verified, the Registrant shall discontinue any business relationship with the customer and consider whether a suspicious transaction or activity report shall be submitted to the FIUTT.

9.10 Irrespective of the size of the transaction, any suspicious activity must be reported to the FIUTT.

Beneficial Ownership

9.11 Where a client/applicant is initiating a business relationship with a Registrant on behalf of another person or entity, the Registrant should identify and verify the identity of the beneficial owner of the account by requesting original identification documents, data or other information where applicable.

9.12 If the beneficial owner is a legal person or arrangement, the Registrant should identify and verify the identity of the natural persons who ultimately own or control the legal persons or arrangements.

9.13 The phrase "ultimately own or control" refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control. Registrants are required to employ reasonable measures to delve into the structure of legal entities, identifying individuals who exert ultimate control over the business and assets. Special attention should be given to scrutinizing shareholders or other entities exercising significant influence over the legal entity's affairs. This diligence is crucial for maintaining transparency, mitigating risks, and upholding the integrity of business operations.

9.14 The Registrant should also ensure that any person purporting to act on behalf of the legal entity is authorized, in writing, to do so (for example, through the company's by-laws, a resolution of the Board of the legal entity, contracts etc.)

9.15 The Registrant should take adequate steps to determine whether a beneficial owner is a PEP and conduct the necessary requirements outlined in Guidelines 9.101 - 9.112.

Enhanced Due Diligence

9.16 Where Registrants have identified higher risks of ML/TF/PF threats, enhanced due diligence measures should be applied. This should include increasing the degree and nature of monitoring of the business relationship with the client to determine whether the transactions and/or activities appear unusual or suspicious.

9.17 The Registrant's policy framework should therefore include a description of the type of clients that are likely to pose higher than average risk and the EDD procedures to be applied in such instances.

9.18 EDD must also be applied in the following circumstances:

a. clients associated with countries that fail to, or insufficiently comply with the FATF Standards;

b. complex, unusual or large transactions, whether completed or not, to all unusual patterns of transactions and to insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
c. where a financial institution determines that a beneficiary who is a legal person or legal arrangement presents a higher risk, the financial institution must identify and verify the identity of the beneficial owner of the beneficiary, at the time of the payout;
d. when establishing counterparty business relationships (e.g. foreign Broker-Dealers, foreign custodians);
e. where the client is a foreign politically exposed person (PEP);
f. where higher risks have been identified with a client who is a domestic PEP or a PEP associated with an international organisation;
g. non face-to-face business relationships or transactions; and
h. in any other situation where money laundering risks are higher.

9.19 The commencement of a business relationship with a PEP must be approved by senior management and such approval must be documented in a manner which can be provided to auditors and Supervisory Authorities upon request.

9.20 Registrants should consider obtaining senior management approval for on-boarding high-risk clients who are not PEPs due to the risk they may pose to the Registrant.

9.21 Registrants should also ensure that monitoring systems are appropriately tailored and provide timely and comprehensive reports to facilitate effective monitoring of business relationships with high-risk clients and periodic reporting on such relationships to senior management and the Board.

Simplified Due Diligence

9.22 Where a Registrant's risk assessment has identified lower ML/TF/PF risks, the Registrant may apply SDD to specifically defined lower risk clients, products and services. SDD should be commensurate with the identified lower risk factors (e.g. the simplified measures may relate to aspects of customer acceptance measures and to aspects of ongoing monitoring).

9.23 The Registrant is required to document its reasons for the application of SDD to the particular client, product and service in a manner which can be produced to the TTSEC upon request.

9.24 It is important to ensure that SDD at account opening provides enough information to be supportive of effective client monitoring. Monitoring will not be effective as a control when a Registrant has too little information about its clients and their expected use of the relevant financial products.

9.25 When utilizing SDD measures to conduct ongoing due diligence Registrants may reduce the frequency of client identification updates and reduce the degree of ongoing monitoring and scrutinizing transactions, based on the monetary thresholds outlined in Regulation 11 of the FORs. Where Registrants choose to do this, they must ensure that the threshold is set at a reasonable level and that systems are in place to identify linked transactions which, when aggregated, exceed the threshold.

9.26 In most cases, the implementation of SDD measures is subject to specific thresholds or restrictions on the type or value of transactions that can be performed. Therefore, ongoing monitoring should allow verification that the transactions remain within the risk-based thresholds and in line with the client's risk profile.

9.27 Registrants must ensure that they have the requisite transaction monitoring infrastructure (i.e. one that would ensure that transactions remain within the risk-based thresholds) in place to adequately perform ongoing due diligence before SDD can be applied. SDD is not an exemption from performing CDD measures but rather, Registrants may adjust the frequency and intensity of measures to satisfy the minimum CDD standards.

9.28 Registrants are reminded that simplified measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or where specific higher risk is determined.

Thresholds for SDD

9.29 Retail and institutional clients with annual sales up to $90,000 annually are subject to SDD requirements once they fall under the following thresholds:

a. Aggregate of all credits does not exceed $90,000 annually;
b. Aggregate of all withdrawals and transfers does not exceed $90,000 annually;
c. Access to debit card, online banking services and ACH services only;
d. International wire transfers are prohibited;
e. Access to credit or overdraft facilities are prohibited;
f. Limited to one business account per person/sole trader either singularly or jointly;
g. Account opening / maintenance fees are not applicable to financial inclusion accounts. ATM and other fees for permissible services (e.g. domestic transfers, purchase of bank drafts) will be applicable.

Simplified Customer Identification Requirements

9.30 The following shall be required for Retail Clients:

a. Obtain one (1) form of valid government issued photo identification of either a passport, national identification card or drivers permit.
b. In respect of a client/applicant who is acting on his own behalf, the minimum relevant documentation should be obtained to ascertain:
    i. Full legal name of the client/applicant;
    ii. Date and Place of Birth;
    iii. Nationality; and
    iv. Permanent address.
    v. Nature, purpose of account, source of funds may be inferred and recorded, e.g. For receipt of pension or social assistance payments and payments of household bills.

9.31 For migrants who cannot satisfy the above requirement for valid national identification, acceptance of a government issued residency card may be considered by registrants.

9.32 The customer must be screened against the lists of designated persons. At a minimum, this should occur at the on-boarding of the customer; when the designated lists are updated;

and on a quarterly basis. Risk-based transaction monitoring controls must be implemented to ensure that the prescribed limits are not breached and that transactions match the initial low-risk profile. At a minimum, these accounts should be reviewed **annually** to determine whether transactional activity is within the established thresholds. Deviations from the established profile, on the basis of risk, should prompt a review of the customer risk rating, noting (d) and (e) in Guideline 9.35 below.

9.33 Full CDD must be carried out in the following instances and in respect of (a) or (b) below, the registrant should consider whether the customer continues to qualify for SDD measures:

a. the customer crosses the established thresholds;
b. the customer wishes to access additional financial services; or
c. where there is suspicion of money laundering or terrorist financing.

9.34 In instances where the above customer due diligence requirements cannot be obtained, registrants must determine whether to continue with the relationship and the Compliance Officer shall determine whether a suspicious transaction or activity report should be filed with the FIUTT.

9.35 The following shall be required for Institutional Clients:

a. Record the customer's full legal name;
b. Complete residential address;
c. Business address [if different from residential address];
d. Nature of business and purpose of account; and
e. Source of funds.

9.36 Record for each individual/owner/partner/director/beneficial owner:

a. Full legal name;
b. Complete residential address;
c. Date and Place of Birth; and
d. Nationality.

9.37 Obtain formation documents/regulating powers, as applicable:

a. Articles of incorporation or continuance;

b. Certification of incorporation;
c. Notice of Directors and Notice of Business Address;
d. Memorandum and Articles of Association; and
e. Partnership agreement.

9.38 Where applicable, obtain:
a. Recent Annual Return
b. National Insurance Board (NIB) Certificate

9.39 Obtain one (1) form of valid government-issued photo identification of either a passport, national identification card, or driver's permit for each individual /owner /partner /director / beneficial owner.

9.40 Screen names of all individuals and the name of the business against lists of designated persons.

See Appendix 5 for examples of SDD measures

Third-Party Reliance

9.41 There may be instances where a Registrant may rely on a third-party financial institution or listed business to perform elements of customer due diligence, in respect of the identification of the customer, identification of the beneficial owner and understanding the nature of the business, or to introduce the business, to avoid duplication and additional costs. For example, when an investment adviser refers business to a broker-dealer or when a Registrant is onboarding a client who has already been onboarded within the financial group to which it belongs. It is important to note that such third-party reliance is subject to regulatory requirements and guidelines. Registrants need to ensure that the third party's due diligence practices align with the applicable legal and regulatory standards. In many cases, there may be specific criteria and agreements in place to govern the reliance on third-party due diligence.

9.42 In such cases, Registrants may rely on third-party financial institutions for performance of the following CDD measures:

a. Identifying the client and verifying that client's identity using reliable, independent source documents, data or information;
b. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the Registrant is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include a Registrant's understanding of the ownership and control structure of the client; and
c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

9.43 Where a Registrant seeks to place reliance on a third-party financial institution to perform elements of CDD, the Registrant must:

a. obtain immediately the necessary information concerning identification of the customer, identification of the beneficial owner and understanding the nature of the business;
b. take steps to satisfy itself that copies of identification data and other relevant documentation relating to customer due diligence requirements will be made available from the third-party financial institution or listed business upon request without delay; and (c) satisfy itself that the third-party financial institution or listed business is:
    i. regulated; or
    ii. supervised or monitored and has measures in place for compliance with CDD and recordkeeping requirements.

9.44 In such instances where third-party reliance is used the ultimate responsibility and accountability remains with the Registrant that is placing reliance on the third-party.

9.45 It is important to note that third-party reliance is different from an introduced business or an outsourcing arrangement. In a third-party reliance scenario, the third-party typically has an existing relationship with the client that is independent of the relationship the client is forming with the relying financial institution.

9.46 The basis for deciding to place reliance on a third-party for CDD must be documented and approved by senior management. Where a third-party financial institution or listed business

is located in another jurisdiction, a Registrant should consider whether the conditions in Guideline 9.44 are met and the level of risk associated with those countries.

9.47 The relationship between Registrants and the third parties relied upon to conduct CDD on their behalf should be governed by a documented agreement between the entities for the exchange of information, e.g. a Service Level Agreement or a Memorandum of Understanding.

9.48 At a minimum, Registrants must be satisfied that the third party:

a. has an adequate CDD process and that information collected clearly establishes the identity of the client or beneficial owner and has been verified;
b. has measures in place for record keeping requirements in accordance with the requirements in AML/CFT legislation and regulations;
c. can provide CDD information and provide copies of the relevant documentation immediately upon request; and
d. is properly regulated and supervised.

9.49 The decision to place reliance on a third-party is not static and should be assessed regularly to ensure that it continues to conduct CDD in a comprehensive manner.

On-Going Due Diligence

9.50 The Registrant should closely monitor the transactions undertaken by its clients through the course of the business relationship to ensure that transactions are consistent with the Registrant's knowledge of its customer, business and risk profile, including, where necessary, the customer's source of funds.

9.51 In addition to obtaining the client's source of funds upon initiation of the business relationship, the Registrant should ensure that documentary evidence of the client's source of funds is obtained for any transaction which falls above the thresholds identified at Guideline 9.26 (whether one-off or not) throughout the business relationship.

9.52 If an existing client can no longer satisfy CDD requirements, the Registrant should consider filing a report with the CO, who should conduct the necessary enquiries to determine whether a SAR should be filed with the FIUTT.

9.53 All documentary evidence of identification requested and obtained from a client as part of a Registrant's CDD policies and procedures must be updated on a frequency dependent upon the Registrant's risk assessment of the client or more frequently as the need arises, for example, on the occurrence of specified events such as changes in name, address, employment or other critical data on the client. See **Appendix 4** for examples of EDD.

CDD for New and Existing Retail Clients

9.54 A Registrant is responsible for verification of the retail client's identity using reliable, independent source documents, data or information prior to establishing a business relationship.

9.55 The identification process should include verification of the client's identity using at least one form of valid picture identification which may be a-

a. passport;
b. national identification card; or
c. drivers' permit.

9.56 Notwithstanding the above, more than one form of picture identification may be requested by the Registrant as part of its EDD measures for higher-risk clients.

9.57 A Registrant is prohibited from opening anonymous accounts or accounts in fictitious names. If a Registrant is unable to verify the true identity of a prospective client or beneficial owner, the Registrant is prohibited from establishing the business relationship. If it is already established, the Registrant must immediately terminate the business relationship. In such a case, the Registrant should immediately file a SAR with the FIUTT.

9.58 In respect of a client/applicant who is acting on his own behalf, relevant documentation should be obtained from the client/applicant to ascertain:

a. Full name of the client/applicant(s);

b. Permanent address and proof thereof;
c. Date and place of birth;
d. Nationality;
e. Place of business/occupation, where applicable;
f. Occupational income, where applicable;
g. Signature of client/applicant(s);
h. Purpose of the proposed business relationship or transaction and source of funds; and
i. Any other information deemed appropriate by the Registrant.

9.59 In respect of a client/applicant who is acting on behalf of another individual, the Registrant should take steps to identify the beneficial owner of the account as set out at Guideline 9.11 and should obtain the relevant documentation which gives the client/applicant the legal authority to act for the beneficial owner such as, but not limited to powers of attorney and letters of authorization.

Verification of Identification

9.60 The verification process for customer identification involves, but is not limited to, reviewing reliable source documentation such as photo identification, birth certificates and other documentation that confirms the necessary information required during the identification process.

9.61 As outlined in Guideline 9.55, a customer's physical identity should be verified using one (1) form of valid picture identification, which may be a valid passport, national identification card or driver's permit. Additional picture identification should be requested by the financial institution only where higher risk is identified and enhanced due diligence is warranted (Guideline 9.56). The Registrant should have measures in place to document the verification of the customer's identity.

9.62 Furthermore, institutions may apply higher standards than those articulated in the Guidelines above based on their risk tolerance and internal policies. Where certain classes of clients, for example, the elderly, the disabled or students are not able to produce the specified types of identification, some measure of flexibility may be afforded, though not so much as to compromise the reliability of the CDD process. The Registrant should

establish internal policies and procedures to facilitate verification of identity in these exceptional circumstances.

Verification of Address

9.63 A client's permanent address may be verified utilizing one or more of the following measures:

a. Obtaining an original recent utility bill (excluding mobile phone bill), tax assessment or bank statement;
b. Reviewing the Register of Electors or any other official Government databases; or
c. Documented record of a home visit.

9.64 Electronic Bills or Paperless Bills are acceptable; however, registrants must ensure that the staff responsible for the onboarding of clients are aware of the appearance and contents of a valid e-bill/paperless bill in order to mitigate the risk of receiving fraudulent documents.

9.65 The documentation obtained to verify the client's permanent address should not be more than six (6) months old, except where verification is conducted using the Register of Electors.

9.66 Where a client's address is temporary accommodation, for example, an expatriate on a short-term assignment, the Registrant should establish internal policies and procedures to obtain verification by other risk-based means, such as a copy of the contract of employment, or banker's or employer's written confirmation.

9.67 Where the utility bill is not in the client's name, the Registrant should request additional information to confirm the client's address such as obtaining a letter from the landlord or a copy of the lease agreement and a recent receipt;

9.68 In the case of students or other young individuals, the Registrant may consider verification using the home address of parent(s) or guardian(s), or by making enquiries with the client's school or university.

Copies of Documents

9.69 Where original identification documents are not available, copies should be acceptable only where the identification can be certified in person. In the case of clients that are not present in Trinidad and Tobago, certification should be done by a Notary Public or a Consulate Office. For clients present in Trinidad and Tobago, certification may be done by a Commissioner of Affidavits. In the case of institutional clients, certification may also be done by way of a Secretarial Certificate.

Applicability of place of business/occupation and occupational income

9.70 The requirement to obtain documentary evidence of a client's place of business or occupational income may be considered not applicable only in circumstances where the prospective client is unemployed, for example:

a. Students;
b. Retirees; or
c. Homemakers.

CDD for New and Existing Institutional Clients

9.71 Registrants must obtain the relevant documentation as outlined in Guideline 9.58, with appropriate adaptations, when onboarding companies, partnerships and sole traders. Examples of appropriate adaptations of Guideline 9.58 for companies would include the company name, registered address and country of incorporation.

9.72 Registrants should implement appropriate adaptations of Guideline 9.58 for self-employed clients who are not able to provide a pay slip or job letters (for example, persons who list "businessman" or "owner" as their occupation). This would include obtaining other forms of documentation to substantiate occupation, such as but not limited to:

a. A taxi badge;
b. Any trade or craftsman's licence or equivalent;
c. Any professional licence or equivalent; or
d. Copies of lease agreements and rental receipts for landlords.

9.73 Registrants should obtain and verify the following additional information, as applicable, when onboarding registered companies and partnerships:

a. Articles of incorporation or continuance;
b. Certificate of incorporation;
c. Company by-laws;
d. Most recent annual return;
e. Partnership deed;
f. Other publicly available documents; and
g. A signed Director's Statement or a certificate by the Company's Secretary outlining the nature of the company's business (this may be obtained from the Company's audited financial statements or other signed declaration from a duly authorized representative of the Company)

9.74 A Registrant should identify and verify the identities of key functionaries of an institutional client using reliable source documents. This information would include, where applicable:

a. Names and identification documents of all Directors, the Company's Secretary, other senior officers and authorized signatories for the account;
b. Names and identification documents for all partners of a partnership; and
c. Sample of signatures.

9.75 In addition to the identification and verification of the institutional client (i.e. registered company, partnership or self-employed person), the Registrant must obtain the following documents to the extent relevant to the proposed business relationship:

a. management accounts for the last three (3) years for self-employed persons and businesses which have been in operation for more than three (3) years; or
b. three (3) year estimates of income for self-employed persons and businesses which have been in operation for less than three (3) years.

9.76 If a prospective institutional client cannot provide the documentation stated at Guideline 9.73 above, the Registrant may request other documentation to prove the source of funds to be used for the transaction such as but not limited to:

a. Rental income earned by a landlord may be substantiated by lease agreements;
b. Deeds to verify ownership of property and bank statements showing earnings from rental; and

c. Other self-employed individuals may produce relevant documentation to substantiate revenue streams including bank statements, invoices etc.).

9.77 For new institutional clients, the following should also be identified and verified, where applicable:

a. Copies of deeds or instruments, Powers of Attorney or other authorities affecting the operation of the account in relation to the business; and
b. Evidence of the authority to enter the business relationship (for example, a copy of the Board Resolution authorizing the investment).

9.78 The frequency of verification and updating of identification documentation for key functionaries of an institutional client should be determined by the entity's risk rating. Higher risk entities should undergo more frequent updates that align with risk mitigation measures.

9.79 Registrants must identify and verify the identity of persons with a substantial interest (10% or more) in the issued and outstanding share capital of the client. This is done to understand the ownership and control structure of the client.

9.80 Information on the purpose and intended nature of the business relationship should be obtained by the Registrant who should also conduct ongoing due diligence with respect to the business relationship.

Foreign Clients

9.81 When engaging in a business relationship with a foreign client, a reference should be sought from the foreign client's bank. In the event a bank reference cannot be obtained, the Registrant should obtain copies or originals of the client's bank statements from its foreign bank. Where copies are obtained, the responsible staff should be aware of the appearance and contents of a valid bank statement to mitigate the risk of receiving fraudulent documents.

Trust Fiduciaries

9.82 Where an applicant for business is a trustee, nominee or other legal arrangement, in addition to the requirements outlined in Regulation 15 of the FORs and in Guideline 9.59 above, the financial institution or listed business shall obtain the following information:

a. Evidence of the appointment of the trustee by means of a certified copy of the Deed of Trust;
b. The nature and purpose of the trust;
c. 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
d. Information on the identity of the beneficiary or class of beneficiaries and verification of this information where available.

9.83 Verification of the identity of a beneficiary of a trust or other legal arrangement shall be performed before the payout or the exercise of vested rights.

9.84 This verification can be established through collecting, at a minimum, the following reliable, independently sourced documents, data or information:

a. A copy of documentation confirming the nature and legal existence of the account holder (e.g. a certified copy of the deed of trust, register of charities);
b. Where the settlor is deceased, written confirmation should be obtained for the source of funds in the form, for example, of a Grant of Probate / Letters of Administration, and/or a copy of the will creating the trust; or
c. Where a corporate trustee acts jointly with a co-trustee, the identity of any non-regulated co-trustees should be verified.

9.85 There may be other procedures of an equivalent nature which may be produced, applied or accessed as satisfactory evidence of a client's identity and risk profile, including:

a. Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
b. Obtaining bank references;
c. Accessing or searching public and private databases or other reliable independent sources.

9.86 Registrants should verify that any person purporting to act on behalf of the legal arrangement is so authorised and, if so, verify not only the identity of that person but also the person's authorisation to act on behalf of the legal arrangement (by means of a signed mandate, a court issued judgment or another equivalent document).

9.87 Depending on the type or nature of the legal arrangement, it may be impractical to verify all persons at the onset of the relationship e.g. in the case of unborn beneficiaries. In such cases, discretion should be exercised. In all circumstances however, there should be verification of beneficiaries before the first distribution of assets. Further, verification of protectors/controllers should be undertaken, either the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of an instruction to an advisor to provide advice.

9.88 Verification should be made to ensure that any bank account on which the trustees have drawn funds is in their names, and the identities of any additional authorized signatories to the bank account should also be verified.

9.89 Further verification of information on the basis of risk, as part of the Registrant's broader customer due diligence measures and ongoing due diligence, should be applied in the context of changes in any of the parties to the trust, revision of the trust, addition of funds, investment of trust funds or distribution of trust assets/provision of benefits out of trust assets, including whether information regarding source of funds and/or destination of funds should be corroborated. Where a trustee whose identity has been verified is replaced, the identity of the new trustee should be verified before the new trustee is allowed to exercise control over funds.

9.90 Any application to open an account, or undertake a transaction, on behalf of another without the applicant identifying a trust or nominee capacity should be regarded as suspicious and requiring further enquiries.

9.91 Institutions should be particularly vigilant where there is no readily apparent connection or relationship between the settlor and the beneficiaries of a trust. Since the economic nature of a trust is a mechanism for the settlor to benefit a beneficiary, typically, not in return for

any consideration (payment, transfer of assets or provision of services), institutions should endeavor so far as reasonably possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. This can be a matter of great sensitivity (for example where the beneficiary turns out to be a child of the settlor born out of wedlock) and institutions are encouraged to take this into account while pursuing necessary or appropriate enquiries.

9.92 There are a number of commercial structures in which a trust may feature as the legal owner, such as structured finance. In such cases where the traditional relationship between the settlor and beneficiary is absent, institutions should demonstrate that they understand the commercial rationale for the arrangement and have verified the identity of the various counterparties.

PEPs

9.93 The FATF defines a PEP as "an individual who is or has been entrusted with a prominent public function". Individuals holding such positions can potentially abuse their power and use his/her influence for the purpose of committing ML offences and related predicate offences, including corruption, bribery, insider trading and market manipulation as well as conducting activity related to TF.

9.94 Regulation 20 of the FORs defines who must be considered a PEP.

9.95 It should also be noted that the family members and close associates of PEPs may also be used to conceal misappropriated funds or assets from abuse of their position or received from corruption or bribery.

9.96 These requirements are designed to be precautionary and should not be misconstrued as labeling all PEPs as being involved in criminal activity. Refusing a business relationship with a PEP simply based on the determination that the client is a PEP would be contrary to the purpose of the Guidelines.

9.97 Registrants must take reasonable measures to determine whether a client is a foreign, domestic or international organisation PEP.

There are three types of PEPs

Foreign PEPs

9.98 Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Domestic PEPs

9.99 Domestic PEPs are individuals who have been entrusted domestically with prominent public functions, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

International Organisation PEPs

9.100 Persons who are or have been entrusted with prominent public functions in an international organisation. This can include officials and executives in international organisations such as the United Nations' six principal organs and multiple specialized agencies, the International Monetary Fund (IMF), the World Bank, and other similar organisations established by international treaties.

9.101 When onboarding a Foreign PEP, the following persons shall be considered high-risk and EDD shall apply to:

a. the foreign PEP;
b. any immediate family members of the foreign PEP, such as the spouse, parent, sibling, children and children of the spouse of the client; and
c. any individual publicly known or actually known to the Registrant to be a close personal or professional associate of the foreign PEP.

9.102 If a client is a Domestic or an international organisation PEP then EDD measures shall only be applied where higher risks are identified to:

a. that client;

b. any immediate family members of that client, such as the spouse, parent, sibling, children and children of the spouse of the client; and
c. any individual publicly or actually known to the Registrant to be a close personal or professional associate of the client.

Steps to be taken regarding PEPs

9.103 Registrants should gather sufficient information about a PEP to understand fully the nature of the PEP's business interests and to determine from publicly available information whether the PEP has been subject to a money laundering or terrorist financing regulatory action.

9.104 Subsequent to determining that the client is a PEP, the Registrant must:

a. ensure that approval is obtained from senior management to establish the business relationship and ensure that such approval is documented;
b. take reasonable measures to establish the source of wealth and source of funds; and
c. conduct enhanced ongoing monitoring of the business relationship. This should include rigorous oversight of PEPs' accounts and EDD measures.

9.105 Registrants should check PEPs' identification against listings available from reputable local and international sources to identify PEPs and to conclude whether there are any red flags a Registrant ought to note in compiling a client risk profile for due diligence.

9.106 Moreover, prior to accepting a PEP as a client, a Registrant should determine whether a PEP is carrying out transactions which originate from or are primarily affiliated with business from countries named on FATF's Public Statements in relation to high risk and other monitored jurisdictions.

9.107 The Registrant's application of due diligence to a client who is no longer entrusted with a prominent public function should be based on the Registrant's assessment of the client's risk and not on prescribed time limits. In this regard, possible risk factors to consider are:

a. The seniority of the position that the individual held as a PEP;

b. Whether the individual's previous and current function are linked in any way (e.g., his involvement in the appointment of his successor);
c. Whether the PEP continues to deal with the same substantive matters and the level of influence that the individual may still exercise.

9.108 Similarly, the period for which family members and close associates of PEPs who have demitted office, should be treated as PEPs, is directly related to the assessment of risk for the primary PEP.

9.109 Registrants should not establish business relationships with PEPs if the financial institution knows or has reason to suspect that the funds are derived from corruption or misuse of public assets.

9.110 Where information collected by Registrants on a PEP cannot be verified or is later determined to be false, the Registrant must immediately discontinue any business relationship with the PEP and report the issue to its CO.

9.111 For additional guidance and information regarding PEPs, see FIUTT's Guidance Note:

AML/CFT Procedures for PEPs.

NPOs

9.112 Given the variety of legal forms that NPOs can have, depending on the country, the FATF has adopted a functional definition of an NPO which is based on those activities and characteristics of an organisation which may put it at risk of TF abuse, rather than on the simple fact that it is operating on a non-profit basis.

9.113 For the purpose of AML/CFT/CPF, NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". Therefore, the measure outlined in the Guidelines applies to those organisations which fall within the FATF definition of an NPO. It does not apply to the entire universe of organisations working in the not-for-profit realm in a country.

9.114 FATF noted that NPOs most at risk of abuse for terrorist financing are primarily engaged in 'service activities'. These are programmes focused mainly on providing housing, social services, education or health care. There is a stronger risk of abuse for NPOs providing services in close proximity to an active terrorist threat such as an NPO operating:

a. In a conflict zone where there is an active terrorist threat; or
b. Domestically in a country where there may not be conflict but is within an area targeted by a terrorist movement for support and cover.

9.115 The Non-Profit Organisations Act No. 7 of 2019 defines an NPO as a body of persons, whether incorporated or unincorporated, which—

a. is established primarily for the promotion of a patriotic, religious, philanthropic, charitable, educational, cultural, scientific, literary, historical, artistic, social, professional, fraternal, sporting or athletic purpose, or some other useful object and raises or disburses funds for that purpose or object;
b. carries on its business without pecuniary gain to its members or officers except as reasonable compensation for services rendered; and
c. restricts the use of any of its profits or other accretions to the promotion of its purpose or object.

9.116 As part of its identity and verification process, Registrants must include in their records evidence that client purporting to operate as an NPO is registered under the appropriate laws and a copy of their registration with the Financial Intelligence Unit of Trinidad and Tobago. For an NPO operating in Trinidad and Tobago, registration is required under the Non-Profit Organisations Act No. 7 of 2019.

9.117 NPOs differ in size, income, structure, legal status, membership and scope and can include research institutes, churches, clubs, and professional associations, community based self-help groups. Generally, NPOs depend in whole or in part on charitable donations and voluntary service for support.

9.118 EDD may not be necessary for all NPO clients as not all NPOs are high risk. Many are small organisations dealing with insignificant donations for redistribution among members.

9.119 Registrants must have measures implemented to determine the level of risk associated with the activities conducted by an NPO client.

9.120 As part of its onboarding and ongoing monitoring activities, Registrants must consider whether funds are being sent to high-risk jurisdictions, whether the NPO client is engaged in activities and have connections that are geographically based near to conflict zones.

Considerations for assessing NPO risk

9.121 To assess the risk of an NPO, a Registrant should consider inter alia:

a. The evidence of registration under applicable laws of the home and local operations;
b. The purpose, ideology or philosophy of the NPO;
c. The geographic areas served (including headquarters and operational areas);
d. Organisational structure;
e. The NPO's donor and volunteer base;
f. Funding and disbursement criteria (including basic beneficiary information);
g. Record keeping requirements;
h. Affiliation with other NPOs, Governments or groups;
i. Identity of all signatories to the account; and
j. Identity of board members and trustees.

9.122 As part of the verification process, Registrants should carry out due diligence against publicly available terrorist lists and monitor on an ongoing basis whether funds are being sent to high-risk countries. Where a non-profit association is registered in an overseas jurisdiction, it may be useful to contact the appropriate charity commission or equivalent body, to confirm the registered number of the charity and to obtain the name and address of the correspondent charity commission for the charity concerned.

9.123 Registrants should satisfy themselves as to the legitimacy of the organisation, by, for example, requesting a copy of the constitution.

9.124 Whilst it is not practical to obtain documentary evidence of identity of all donors, where possible, Registrants should undertake a basic level of due diligence of a foreign NPO's donors in relation to known ML/TF/PF activities.

Cross-Border Relationships

9.125 In relation to cross-border relationships with counterparties (e.g. foreign Broker-Dealers, foreign custodians) and in addition to performing its normal due diligence measures, Registrants should:

a. Gather sufficient information about a counterparty such as incorporation documents, names of the beneficial owner/s and directors, audited financial statements (if available) and other pertinent documents to understand fully the nature of its business and to determine from publicly available information the reputation of the counterparty and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigations or regulatory action.
b. Assess the counterparty's anti-money laundering and terrorist financing controls;
c. Obtain approval from the CO or relevant senior officer before establishing new counterparty relationships; and
d. Document the respective responsibilities of the Registrant and counterparty.

9.126 Where Registrants have a cross-border relationship with a counterparty which permits clients of the Registrant to use the counterparty's accounts to conduct securities transactions on the client's own behalf, the Registrant must satisfy itself:

a. That it has performed CDD obligations on its clients that have direct access to the accounts of the counterparty; and
b. That it can provide relevant CDD information upon request to the counterparty.

9.127 Registrants should not enter or continue a counterparty relationship with a financial institution incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks).

Non-Face-to-Face Clients

9.128 FATF Recommendation 10 requires regulated entities to use a risk-based approach (RBA) to determine the extent of the CDD measures to be applied, however, Recommendation 10 includes "non-face-to-face business relationships or transactions" as an example of a potentially higher-risk situation in undertaking CDD. The POCA and the FORs identify

non-face-to-face business relationships or transactions as high risk to which EDD must be applied.

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

9.130 Where verification of identity is performed without face-to-face contact (e.g. via the internet), additional checks should be applied to manage the risk of fraud. Examples of such procedures may include, but are not limited to:

a. **Document authentication:** Verify identity documents using technologies that check for security features or use a reliable, independent source to confirm data.
b. **Digital identity:** Use secure digital identity systems, which can include biometric data from passports or other secure electronic methods.
c. **Third-party verification:** If a third party is involved, obtain the client's consent and verify the third party's identity.
d. Telephone contact with the customer at a residential or business number that can be independently verified;
e. Confirmation of the customer's address through an exchange of correspondence or any other appropriate method;
f. Telephone confirmation of the customer's employment status with his employer's human resource department at a listed business number of the employer; or
g. Confirmation of the customer's income details by requiring the presentation of a recent job letter or bank statement, where applicable.

9.131 Where it is impractical or impossible to obtain original documents for identification purposes, a legible copy can be accepted as suitable evidence of identity provided that the copy has been certified by a recognized notary public or consular office as being a true copy of the original document and the photo is a true likeness of the client.

9.132 The Registrant must ensure that the notary public or representative of consular office has signed the copy document (printing his name clearly underneath) and has also clearly indicated his/her position or capacity, together with appropriate contact information, including an address and a phone number.

9.133 In the case of a person from a country that is deemed "high-risk", the Registrant should contact appropriate foreign authorities to verify identification information (e.g. Government Agencies or Consular Office).

9.134 Registrants should exercise due caution if entering into business relationships or otherwise doing business with persons from high-risk jurisdictions named in Public Statements issued by the FATF, CFATF and FATF styled regional bodies.

Information Sharing

9.135 Regulation 7 (4) and 7 (4A) of the FORs guides Registrants in establishing a group-wide compliance programme, which should include policies, procedures and controls for sharing information between branches and subsidiaries for the purposes of customer due diligence and money laundering risk management. Also, information and analysis of transactions or activities which appear unusual, where such analysis was done.

9.136 Where appropriate and practical and where there are no data protection restrictions, Registrants should take reasonable steps to ensure that customer due diligence information is available throughout all divisions of the business.

9.137 The availability and use of other financial information held is important for reducing the additional costs of collecting customer due diligence information and can help increase a Registrant's understanding of the risk associated with the business relationship.

9.138 Registrants are required to have appropriate risk management systems and procedures in place to identify when their client (or the beneficial owner of the account or of an institutional client) is a PEP and to manage any elevated risks.

10. PART 4: WIRE TRANSFERS

10.1 It is imperative that Registrants are aware of the ML/TF/PF risks inherent in facilitating wire transfers on behalf of others. Registrants are therefore required to maintain policies

and procedures for facilitating wire transfers and incorporate this into their AML/CFT/PF compliance programme.

10.2 While effecting wire transfers are under the remit of commercial banks, Registrants have an obligation to keep sufficient records to substantiate the originator, and beneficiary of the wire transmission.

10.3 These records should be kept in a format which enables them to be produced immediately to the FIUTT and the TTSEC upon request.

10.4 Although the wire transfer may originate from the Registrant's accounts held at commercial banks, when the Registrant is ordering a wire transfer on behalf of a client, identification data regarding the underlying client and recipient of the funds should be included in the wire transmission.

10.5 These Guidelines on wire transfers aim to ensure basic information on:

a. the originator;
b. the underlying client on whose behalf the wire is being transmitted; and
c. the beneficiary of the wire transmission.

10.6 The basic information is immediately available:

a. To Registrants to facilitate the identification and reporting of suspicious transactions;
b. To the FIUTT for analyzing suspicious activity and disseminating as necessary; and
c. To law enforcement and/or prosecutorial authorities to assist in detecting, investigating, prosecuting terrorists or other criminals and in tracing the assets of the said terrorists or other criminals.

10.7 In relation to outgoing wire transfers, Registrants should maintain records of the following:

a. The instruction from the client to transact the wire transfer on the client's behalf;
b. The instruction sent to the Registrant's bank to affect the wire transfer; and
c. The advice from the bank that the wire transfer was completed (if conducted on an online platform, a "screenshot" of the completed transaction would suffice).

Domestic and Cross-Border Wire Transfers

10.8 Domestic and Cross-border wire transfers should be accompanied by accurate and meaningful identification data on the originator of the transfer. Wire transfers must always contain:

a. The name of the originator of the transfer;
b. The address or national identification number or a passport number of the originator;
c. The account number of the originator, and in the absence of an account, a unique transaction reference number which permits tracing of the transaction;
d. The name of the beneficiary; and
e. The beneficiary account number where the account is used to process the transactions, or in the absence of an account, a unique transaction number which permits tracing of the transaction.

10.9 Registrants should be able to identify wire transfers lacking complete originator information, so that the lack of complete information will be considered as a factor in assessing whether a wire transfer is, or related transactions are suspicious and require reporting to the FIUTT.

10.10 Registrants should have a process in place to verify the identity of the beneficiary for wire transfers in excess of six thousand dollars and maintain a record of such verification.

11. PART 5: RECORD KEEPING REQUIREMENTS

11.1 The following Guidelines should be incorporated into a Registrant's document retention policy which would allow for provision of information to auditors and other supervisory authorities, law enforcement authorities and any other competent authority with the authority to request such records.

Retention Period

11.2 Registrants must retain records as outlined in Regulation 31 (1) of the FORs and containing the information as required, as per Regulation 32 (1), in either written or electronic form for a minimum period of six (6) years.

11.3 A Registrant is required to maintain records on both domestic and international transactions for a period of at least six (6) years in the following circumstances-

a. In the case of a Registrant and a client which continues to maintain a business relationship, from the date of the completion of the last transaction;
b. In the case of a Registrant and a client who have formed a business relationship, from the date on which that relationship ends; or
c. In the case of a one-off transaction or a series of such transactions, from the date of completion of the transaction or the date of the last transaction in a series.

11.4 Customer identification information for clients of a Registrant who continue to maintain a business relationship with the Registrant must be retained, maintained and updated throughout the business relationship.

Extension of Retention Period

11.5 Notwithstanding Guideline 11.2-11.4 above, the TTSEC or the FIUTT may extend the requirement of retaining records beyond the stipulated six (6) year period.

11.6 Where there has been a report of a suspicious activity via a SAR or where there is an ongoing investigation by the FIUTT or a competent law enforcement authority into money laundering and/or terrorist financing, records relating to the transaction for the investigated parties should be retained until confirmation is received that the matter has been concluded or the market actor has otherwise been advised by the FIUTT or a Court of competent jurisdiction that it is safe to dispose of these records.

11.7 A Registrant must keep the transaction records in such format which may include –

a. Electronic;
b. Print;

c. Microfilm; or
d. Such other format as may be specified from time to time by either the TTSEC or the FIUTT.
e. These records should contain sufficient details to permit the reconstruction of a specific transaction.

Requirement to make records available

11.8 A Registrant must make available at the request of the TTSEC, any other Supervisory Authority or Law enforcement authorities, records retained in accordance with the Guidelines.

11.9 Records should contain the following data as outlined in Regulation 32(1) of the FORs-

a. Details of transactions, whether domestic or international including the amount and type of the currency used, account files and business correspondences;
b. A copy of any documentation utilized in the CDD process;
c. The results of any analysis undertaken related to the course of a business relationship or a one-off transaction; and
d. The identification documentation an address of the place where a copy of that evidence may be obtained.

11.10 When a Registrant merges or acquires another organisation, it should ensure that the records such as CDD, transactions, external audit and training can be readily retrieved. Where the records are kept in a contractual relationship by an entity other than the Registrant, the Registrant is responsible for retrieving those records before the end of the contractual arrangement.

11.11 Each Registrant is required to maintain a register of all enquiries containing the date and nature of the enquiry; the name and agency of the enquiring officer; and the powers being exercised. This register should be kept separate from other records.

12. PART 6: SUSPICIOUS ACTIVITY / TRANSACTION REPORTING

12.1 If a Registrant suspects or has reasonable grounds to suspect that the client's funds are the proceeds of criminal activity or are related to terrorist financing, the Registrant must file a Suspicious Activity / Transaction Report with the FIUTT as soon as possible, but in any event, within five (5) days of the date from which the Registrant knew or had reasonable grounds to suspect that the client's funds are the proceeds of criminal conduct.

Suspicious Activity

12.2 In determining what constitutes a suspicious activity or a suspicious transaction a Registrant must pay special attention to all-

a. Complex, unusual, large transactions whether completed or not, and all unusual patterns of transactions and to insignificant but periodic transactions, which have no apparent economic or lawful purpose; and
b. Business transactions between individuals, corporate persons and financial institutions in or from other countries which do not comply with, or who comply insufficiently with the recommendations of the FATF.

Transaction Monitoring

12.3 A Registrant is required to pay special attention to the transactions outlined under Guideline 12.2 (Suspicious Activity) by having policies, procedures and systems in place for transaction monitoring.

12.4 Transaction monitoring should be conducted using a risk-based approach which is consistent with the client's risk profile and the Registrant's business operations.

12.5 Registrants should note that it is insufficient to monitor only large transactions given that this would not adequately mitigate risks posed by complex, unusual large transactions, whether completed or not, unusual patterns of transaction and insignificant but periodic transactions which have no apparent economic or visible lawful purpose as required by section 55(2)(a)(ii) of POCA. Transaction monitoring policies and procedures should allow

Registrants to detect structuring of transactions in one account as well as across more than one related account such as accounts that have the same beneficial owner or accounts in the name of clients who are related or close associates.

12.6 Registrants must have policies, procedures and systems in place to monitor clients based on:

a. The client's normal course of dealings with the Registrant to enable the Registrant to detect unusual transactions or patterns of transactions relative to what has been determined to be the expected activity of the client;
b. Known ML/TF/PF typologies in the securities industry.

12.7 The degree of monitoring should be in line with the customer's risk rating.

12.8 Monitoring can be conducted either in real time or after the transaction has taken place through an independent review of the transaction and/or series of transactions. However, this should be undertaken within a reasonable time frame, depending on the risk rating applied to the client.

12.9 Transaction monitoring systems may be automated or manual depending on the size, volume and complexity of the Registrant's business operations.

12.10 The parameters and thresholds used to generate alerts of unusual transactions/activity should be customized to be commensurate with a Registrant's ML/TF/PF risk profile and the complexity and extent of its business activities.

a. Standard parameters provided by the vendor may be used but the Registrant must be able to validate and demonstrate to the TTSEC that these are appropriate for the institution's risk position.
b. The monitoring system should be tested on a periodic basis to ensure that the parameters are performing as expected and remain relevant.
c. Modifications may be required as a result of the testing outlined in Guideline 8.42-8.53. Findings, analysis and the proposed modifications should be documented indicating:
    i. The rationale for reviewing the parameters and thresholds;
    ii. Details of testing; any assumptions made and the analysis of outcomes; and

iii. The changes made to the parameters and thresholds.

12.11 The monitoring system should enable registrants to monitor and report to senior management on all customer relationships and identify activities that are inconsistent with the registrant's knowledge of the customer, their business and risk profile.

Training to Identify Suspicious Activity

12.12 Staff at all levels must be trained at least ***once annually,*** as outlined in Guideline 8.37 (Education and Training), to identify suspicious activity and must be aware of the proper procedure to be followed when suspicious activity is detected. A non-exhaustive list of indicators of Suspicious Activity can be found in **Appendix 2** of the Guidelines.

Suspicious Activity / Transaction Reporting

12.13 A Registrant's staff must report all suspicious activities or transactions to the CO immediately upon detection.

12.14 In instances where a Registrant suspects or has reasonable grounds to suspect that ML/TF/PF activity occurred, the Registrant must initiate, conduct and finalize its examination of such activities/transactions within a reasonable time frame.

12.15 A CO who knows, suspects or has reasonable grounds to suspect that-

a. a customer's funds represent proceeds of criminal conduct; or
b. that a transaction or activity appears to be suspicious, should report his suspicions as soon as possible but no later than five (5) days from the date the transaction was found to be suspicious to the FIUTT in the form of a SAR/STR in accordance with the FIUTT Regulations.

12.16 Registrants should implement a process for recording 'not filed' (closed, not suspicious) internal SAR/STR which should be maintained and recorded by the CO.

12.17 Where a SAR/STR has been filed with the FIUTT, Registrants should continue to monitor and report any further suspicious or unusual activity in relation to that client's accounts.

12.18 A Registrant and/or its staff must not disclose the existence, submission or content of a SAR/STR to any person, either directly or indirectly as this would amount to an offence of tipping off. For example, the termination of a business relationship with a client without due cause may result in tipping off the client that a SAR was filed (section 55A(2) of the POCA refers).

12.19 Where a Registrant is part of a financial group with common clients, consideration should be given to the Registrant's risk exposure and as far as possible information on clients should be shared to ensure that all facts are considered, and consistent decisions are made at group wide level. Such instances must immediately be brought to the attention of the Group CO.

12.20 Where a client is unwilling or unable to provide the necessary due diligence information and/or documentation in opening an account or in completing a transaction, a Registrant should not commence the business relationship or perform the transaction and/or terminate the business relationship and submit a report to the CO.

12.21 On receipt of the report the CO must consider submitting a SAR/STR to the FIUTT.

12.22 A Registrant should keep copies of all reports made to the FIUTT with respect to suspicious customer activity for a minimum of six (6) years.

Register of Enquiries

12.23 A Registrant should maintain a register of all enquiries made to them by any law enforcement authority, Supervisory Authority or other local or foreign authorities acting under powers provided by the relevant laws or their foreign equivalent.

12.24 The register in Guideline 12.23 should be maintained for a minimum of six (6) years and be kept separate from other SAR/STR records.

12.25 The register in Guideline 12.23 should contain at minimum the following information:

a. The date and nature of the enquiry;

b. The name and agency of the enquiring authority; and
c. The power(s) under which the request was being made.

Tipping-off

12.26 Where a Registrant suspects that ML/TF/PF has occurred in respect of one of its clients and the Registrant reasonably believes that if the CDD process is carried out, the client will be tipped-off, the Registrant shall file SAR/STR with the FIUTT instead of performing the CDD or EDD process.

12.27 A Registrant should take great care to ensure that the client does not become aware that his activities have been reported to the FIUTT in circumstances where a SAR/STR has been already submitted to the FIUTT, and it becomes necessary to make further enquiries.

12.28 A person who knows or suspects that an investigation is being or is about to be carried out by law enforcement authorities or supervisory authorities, must not disclose to any person information or any other matter that is likely to prejudice the investigation or proposed investigation.

12.29 A Registrant must not disclose to their client that it has reported, or intends to report, any transactions, or activity to the FIUTT.

13. PART 7: TERRORIST FINANCING

13.1 FATF Recommendation 6 reinforces the principles established under UNSCR 1267 (1999) and UNSCR 1373, which require countries to freeze without delay[7], the funds or assets, and to ensure that no funds and other assets are made available to or for the benefit of, persons or entities designated under such lists.

13.2 In Trinidad and Tobago, the Financial Intelligence Unit (FIUTT) is the primary authority for setting operational protocols for sanctions screening. The protocols are based on a risk-

[7] The term 'without delay' ideally means within a matter of hours of designation by the UNSC or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee)

based approach and are mandatory for all "Reporting Entities," which include financial institutions and listed businesses.

13.3 The Anti-Terrorism Act **(Section 22A(1) of the ATA)** designates the financing of terrorism as a criminal offence. Financing of terrorism refers to the direct or indirect, willful provision or collection of funds, or coercing, encouraging, enticing, or inciting another person to do so, without lawful excuse, with the intention or in the knowledge that such funds are to be used in whole or in part—

a. in order to carry out a terrorist act;
b. by a terrorist;
c. by a terrorist organisation;
d. in order to facilitate travel by an individual to a foreign State for the purposes of—
    i. carrying out a terrorist act; or
    ii. participating in, or providing instruction or training to carry out a terrorist act;
e. by a listed entity; or
f. to facilitate the travel or activities of a foreign terrorist fighter.

13.4 There are several risk factors that a Registrant should consider when assessing their risk exposure to the financing of terrorism. A non-exhaustive list of such risk factors and indicators of terrorist financing can be found at **Appendix 3**.

13.5 Registrants shall be responsible for screening clients against the UNSCR 1267 (1999), 1988 and UNSCR 1373 lists of designated persons and entities and list of persons or entities designated by the High Court of Trinidad and Tobago (also known as the Consolidated List), all of which shall be circulated by the FIUTT in accordance with Section 22AA(2) of the ATA, at the time of onboarding and on an ongoing basis. Evidence of such screening shall be maintained by the Registrant and be provided to the Supervisory Authority upon request.

13.6 A Registrant must comply with Section 22AB of the ATA by following the procedures listed below upon checking the lists as stated in Guideline 13.5 above:

a. Registrants must immediately inform the FIUTT, by using the prescribed form on the FIUTT website[8], if any person or entity named on the lists has funds or accounts with the Registrant;
b. If a Registrant has reasonable grounds to believe that a person or entity named on the lists has funds within Trinidad and Tobago, the Registrant must immediately inform the FIUTT using the prescribed form which can be found on the FIUTT website;
c. If a person or entity named on the lists attempts to enter into a transaction or continue a business relationship with the Registrant, the Registrant must immediately submit a SAR to the FIUTT and:
    i. must not enter into the transaction and/or business relationship; and
    ii. must cease to continue the transaction and/or business relationship with that person or entity and freeze the funds held in the person's or entity's account.

13.7 Registrants shall have procedures to delist and unfreeze funds and assets of persons and entities, should a person or entity no longer meet the requirements for listing on the Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) List or the 1988 List, pursuant to section 22BD(3) of the ATA.

14. PART 8: PROLIFERATION FINANCING

14.1 FATF Recommendation 7 places obligations on countries to comply with all United Nations Security Council Resolutions to apply targeted financial sanctions relating to the financing of the proliferation of weapons of mass destruction.

14.2 On December 14, 2018, two pieces of subsidiary legislation[9] (Legal Notice No. 184 of 2018 and Legal Notice No.185 of 2018), respectively, were enacted by the President of Trinidad and Tobago in accordance with section 4 of the Economic Sanctions Act, Chap. 81:05.

[8] https://fiu.gov.tt/wp-content/uploads/22_Apr_22_Terrorist-Funds-Report.pdf
[9] The Economic Sanctions (Implementation of United Nations Resolutions on the Democratic People's Republic of Korea) Order, 2018, ("the DPRK Order") (by Legal Notice No.184 of 2018); and The Economic Sanctions (Implementation of United Nations Resolutions on the Islamic Republic of Iran) Order, 2018 ("the Iran Order") (by Legal Notice No. 185 of 2018). Update: Re-application of UN Security Council Resolutions related to Iran

14.3 Legal Notice No. 43 of 2019 and Legal Notice No. 44 of 2019 pursuant to section 4(5) of the Economic Sanctions Act Chap. 81:05 enact the Iran and DPRK Orders in Trinidad and Tobago made pursuant to FATF Recommendation 7 and the United Nations Security Council Resolutions. The Orders can be found at: https://www.un.org/securitycouncil/content/un-sc-consolidated-list. Following the activation of the Snapback Mechanism under United Nations Security Council Resolution (UNSCR) 2231 (2015), all provisions of UNSCRs 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), and 1929 (2010) related to Iran were re-instated with effect from 27 September 2025. This includes the targeted financial sanctions imposed under UNSCRs 1737, 1747, 1803, and 1929.

14.4 The Office of the Attorney General and Ministry of Legal Affairs publishes on its website every order obtained from the High Court under the Iran and DPRK Orders in respect of listed entities or related persons. This includes freezing orders, amendments to such orders and revocations of such orders. The Attorney General also publishes each such order in the Gazette and two daily newspapers within seven (7) days of the order being granted.

14.5 The role of the Registrant is to implement controls to prevent access to financing by individuals and entities who may be involved in or supporting such proliferation. Registrants' AML/CFT/CPF compliance programmes shall include PF controls, such as screening against the applicable UN lists of designated persons and countries.

14.6 The Iran and DPRK Orders establish a judicial mechanism by which specific persons and entities involved in or related to the WMD programmes of Iran and DPRK are identified ("listed entities[10]"); their property is frozen; their access to property is otherwise restricted; and they are denied access to the financial system. To achieve this the Iran and DPRK

[10] The United Nations Security Council publishes two lists identifying persons and entities who are involved in or are related to the WMD programmes of Iran and DPRK prohibited by the United Nations:

- "The 2231 List" for Iran which can be found at the following link: https://www.un.org/securitycouncil/content/2231/list. All the persons and entities on the 2231 List are "listed entities" for the purposes of the Iran Order; and
- "The 1718 List" for DPRK which can be found at the following link: https://www.un.org/securitycouncil/sanctions/1718/materials. All the persons and entities on the 1718 List are "listed entities" for the purposes of the DPRK Order.

The UN regularly updates these lists with additional identifier information about each listed entity as it becomes available.

Orders also set out prohibitions with respect to members of the public dealing with such listed entities or their property.

14.7 Registrants **MUST** immediately inform the FIUTT where any of the following apply-

a. They have knowledge or reasonably suspect that any entity named in the Court Order has property or funds within the Financial Institution or Listed Business; or

b. There is a transaction being conducted by a person involving property or funds owned or controlled, whether directly or indirectly, by an entity named in the Court Order in the form made by the Economic Sanctions Act, Chap 81:05.

APPENDIX I

Key characteristics of the securities sector and products which make it more vulnerable to ML/TF/PF abuse.

i. Securities products can be utilised in the layering and integration stages of money laundering once illicit assets are placed in the financial system. However, the securities industry is not generally favourable to placement of illicit assets into the financial system. Nevertheless, certain securities products do pose identifiable ML/TF/PF vulnerabilities even at the placement stage and illicit proceeds may directly be placed for buying securities.

ii. The structure of the securities sector and the variety of intermediary roles does not allow for a one-size-fits-all AML/CFT/CPF approach. Therefore, the structure and variety highlight the importance of Registrants' understanding of their ML/TF/PF risks both directly (e.g., through transactions executed by customers) and indirectly (e.g., risks associated with the underlying customers of the securities provider's customers, or risks associated with the possibility that an intermediary or other entity on which the securities provider relies to perform a task fails to do so). Registrants should implement risk sensitive measures to mitigate the ML/TF/PF risk faced by them.

Broker- dealers

i. One of the most active participants in the securities market is the brokers or dealers in securities. Important to note is that it remains the responsibility of each institution to ensure that the proper CDD process has been completed. A specific vulnerability associated with broker-dealers is their reliance on another financial institution's CDD process. A broker-dealer may assume because another reporting entity has opened an account for a customer, the customer does not pose ML/TF/PF risks for them. The CDD vulnerability is most problematic in relation to the funding of a securities account. If illicit assets are successfully placed at a depository institution, the broker-dealer may assume that, because the funds are from an institution which is subject to AML/CFT/CPF laws, the customer does not pose a ML/TF/PF risk and therefore may accept cheques from that institution to fund a securities account. Once a securities account is funded, a customer can engage in a number of

transactions that further conceal the source of his or her illicit funds, thereby successfully layering and integrating illicit assets that were placed through a depository institution.

Asset Managers, Custodians, and Portfolio Managers

i. Brokers and dealers in securities can be distinguished from those securities intermediaries that are regulated as asset managers, custodian and portfolio managers. The roles of a broker and a dealer are clearly delineated from those of custodian or managers; however, their functions can be housed in the same entity by means of multiple registrations / roles / functions. Also, such advisory functions and broker-dealer functions may be conducted under the same registration. Role of the asset manager, custodian and portfolio manager is generally to advise on the composition of an investment portfolio or to hold securities of local or foreign customers or to manage the contents of investment accounts for retail or institutional customers respectively. Portfolio management typically involves the provision of financial services in a managed relationship with customers who are often of high net worth. The value and type of products offered to high-net-worth customers, together with the international nature of the business, make the provision of wealth management services potentially attractive to money launderers, to disguise their illicit assets. Custodians are essential for the safekeeping of financial assets, and they play a critical role in maintaining the integrity of the financial system. It is important to note that the risks associated with custodian services are generally lower compared to services directly involved in making investment decisions or actively managing funds. While custodian services themselves are not typically used for ML, they may become part of a larger ML scheme due to the nature of their role in the financial system.

Shell Companies

i. The term “shell company” often refers to a non-publicly traded corporation or limited liability company that might have no physical presence and generates little or no independent economic value. These companies are commonly organised in a way that makes their ownership and transaction information easier to conceal. Thus, transactions involving shell companies present a high ML/TF/PF vulnerability. Whilst publicly traded shell companies can be used for illicit purposes, ML/TF/PF vulnerabilities associated with shell companies are heightened when the company is privately held, such that beneficial

ownership can be more readily obscured. For example, a domestic or international shell company securities account can be used to evade CDD investigations regarding the beneficial owners of certain assets. In particular, individuals or entities in high-risk areas/jurisdictions can disguise their true identities through a series of shell companies located in various jurisdictions to participate in a financial system that they otherwise would not be able to access.

ii. Shell companies can also be used to introduce illicit funds into a financial system and/or generate illicit funds through manipulative or fraudulent securities activities. For example, a brokerage account can be opened in the name of shell companies and used to engage in fraudulent conduct with regard to low priced, illiquid, low volume or privately placed securities. In addition, a shell company can be established to accept payments from criminal organisations for non-existent services. These payments, which appear legitimate, can be deposited into depository or brokerage accounts and used to purchase securities products that are easily transferable or redeemable.

Cheques

i. Cheques can be used to fund securities accounts with a securities intermediary. In addition, the use of cheques is not limited to those drawn from a depository account but also can involve pay order/bank draft. Money launderers can purchase pay orders/bank draft, pay order with cash over a period of time or through a series of transactions in order to avoid threshold currency reporting requirements. These cheques can then be deposited into securities accounts until a desired amount is reached and used to purchase a security, which is then sold or transferred. Cheques from a depository account also present ML/TF/PF vulnerability because they may affect the securities intermediary's risk analysis, in particular with respect to CDD obligations. For example, if a cheque originates from another reporting entity subject to an AML/CFT regulatory regime, a securities firm may not conduct a thorough CDD investigation because it believes that the originating reporting entity has already conducted its own CDD investigation, or because the firm perceives a reduced risk because the customer was able to open an account at another financial institution. This vulnerability can become systemic if numerous securities intermediaries perceive a reduced risk based on the activities of others. In addition, even if the reporting entity from which the cheque originated has conducted thorough CDD and not detected anything suspicious, there

may still be an ML/TF/PF risk that the securities intermediary, through its own knowledge of the investor, may be in a unique position to identify. In particular, CDD does not only involve mere customer identification but establishing the purpose and intended nature of the business relationship.

Insider Trading

i. Insider trading involves situations where an insider, who buys and sells securities, whilst in possession of material, non-public information about the security. This includes situations where a person in possession of material, non-public information provides this information to someone else for trading where, depending on the circumstances, the recipient of the information can violate insider trading laws as well. Insider trading is unique to the securities industry and generates illicit assets. As a predicate offence for money laundering this type of misconduct is reportable as STR to the FIUTT. The illicit assets generated by insider trading can be laundered through the securities industry itself or through other parts of the financial sector. The most common example of using insider trading to launder funds would be the simple transfer of illicit proceeds to a bank account.

Market Manipulation

i. Market manipulation generally refers to conduct that is intended to deceive investors by controlling or artificially affecting the market for a security. In particular, the manipulator's purpose is to drive the price of a security up or down in order to profit from price differentials. There are a number of methods that manipulators use to achieve these results. The most pervasive market manipulation method involves what is referred to as a "pump-and-dump" scheme. This scheme involves touting a company's stock with false or misleading statements, often in conjunction with securities trades that raise the price of the security or make it appear as if the securities trading volume is higher than it actually is. Therefore, the price of the security is artificially raised ("pumped"); the security is then sold ("dumped") for a profit. Often the underlying security is low priced, illiquid, and trades with little volume. Another most used method is circular trading, where a trader or group of traders artificially inflates the trading volume of a security by buying and selling it among themselves, creating a misleading impression of market activity and giving the appearance of increased demand or liquidity.

Securities Fraud

i. Securities fraud broadly refers to deceptive practices in connection with buying and selling of securities. In this regard, securities fraud encompasses insider trading and market manipulation activities and poses significant ML/TF/PF risks for the market intermediaries.

ii. *Other characteristics of the securities sector which makes it more vulnerable to ML/TF/PF abuse:*

   a. *Complex Transactions*: Securities transactions can involve complex structures and multiple parties, making it challenging to trace the origin and movement of funds. This complexity can be exploited by individuals seeking to conceal illicit activities;

   b. *Use of Derivatives and Complex Financial Instruments*: The use of derivatives and other complex financial instruments in the securities sector can create opportunities for abuse. These instruments can be exploited to obscure the true nature of financial transactions;

   c. *Anonymity and Pseudonymity*: Certain securities transactions may allow for a degree of anonymity, especially in the case of nominee accounts or shell companies. This anonymity provides opportunities for criminals to disguise their identities and the true purpose of financial transactions;

   d. *High Transaction Volumes*: The securities sector can experience high transaction volumes, which may make it more challenging for financial institutions to identify suspicious patterns amid the sheer volume of legitimate transactions;

   e. *Electronic Trading Platforms*: The use of electronic trading platforms introduces additional vulnerabilities, as cybercriminals may attempt to exploit weaknesses in cybersecurity to facilitate illicit activities, including ML/TF/PF. Transactions executed both on registered securities exchanges and elsewhere, such as over-the-counter transactions (where parties trade bilaterally), and reliance on alternative trading platforms, electronic communication networks and internet-based trading;

   f. *Lack of Beneficial Ownership Transparency*: In some jurisdictions, there may be a lack of transparency regarding beneficial ownership of securities. This opacity can be exploited by criminals to hide their involvement and ownership interests in securities;

   g. *Custodial Arrangements*: Securities are often held in custodial arrangements, and the movement of assets between custodians can be complex. Criminals may attempt to exploit these arrangements to obscure the beneficial ownership of assets;

   h. *Differences among jurisdictions* in terms of defining securities, securities products and services and their providers and the AML/CFT regulated status of these providers;

i. ML/TF/PF risks stem mainly from types of securities products and services, customers, investors and payment methods used in the securities sector; noting that cash is generally not accepted by securities providers in many jurisdictions;
j. *Global reach of the securities sector* and speed of transactions across a multitude of onshore/offshore jurisdictions and financial markets;
k. *High liquidity of certain securities products* can introduce specific ML/TF/PF risks due to the ease with which these products can be converted to cash;
l. Common involvement of a multitude of securities providers and intermediaries on behalf of both buying and selling principals or agents;
m. *An often highly competitive* and sometimes incentive-driven environment, which may lead to a higher appetite for risk, or failure to adhere to internal controls;
n. *Complex products* that may be offered before they are regulated (or not regulated at all), before they are rated for ML/TF/PF risks (e.g. the crypto-assets); and
o. *Challenges in setting the price* for some securities products due to their bespoke nature or complexity, also pricing volatility of some products, particularly low-priced securities.

APPENDIX II

INDICATORS OF SUSPICIOUS ACTIVITY

Money launderers are always developing new techniques; therefore, no list of suspicious indicators can be fully comprehensive. However, the following list provides some key factors that may heighten a client's risk profile or indicate to the Registrant the need to exercise caution and be vigilant.

CDD/KYC

i. The client provides the securities firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the client has provided. This indicator may apply to account openings and to interaction subsequent to account opening, such as wire transfers.

ii. During the account opening process, the client refuses to provide information to complete CDD/KYC (e.g. occupation, prior financial relationships, etc.).

iii. The client, whether a person or entity, is reluctant to provide the securities firm with complete information about the nature and purpose of the client's business, prior financial relationships, anticipated account activity, the entity's officers and directors or business location.

iv. The client, whether a person or entity, is located in a jurisdiction that is known as a bank secrecy haven, a tax shelter, or high-risk geographic locations (e.g. narcotics producing jurisdiction).

v. The client is reluctant to meet personnel from the securities firm in person, is very secretive and/or evasive or becomes defensive when asked to provide more information.

vi. The client refuses to identify a legitimate source of funds or provides the securities firm with information that is false, misleading, or substantially incorrect.

vii. The client engages in frequent transactions with money services businesses.

viii. The client's background, whether a person or entity, is questionable or does not meet expectations based on business activities.

ix. The client has no discernible reason for using the firm's service or the firm's location (e.g. client lacks roots in the local community or has come out of his or her way to use the firm).

x. The client refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, misleading or substantially incorrect.

xi. The client's address is associated with multiple other accounts that do not appear to be related.

xii. The client has a history of changing financial advisors and/or using multiple firms or banks. This indicator is heightened when the client uses firms located in numerous jurisdictions.

xiii. The client is known to be experiencing extreme financial difficulties.

xiv. The client is, or is associated with, a PEP or senior political figure.

xv. The client refuses to invest in more appropriate securities when those securities would require a more enhanced CDD/KYC procedure.

xvi. The client with a significant history with the securities firm abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction.

xvii. The client appears to be acting as a fiduciary for someone else but is reluctant to provide more information regarding for whom he or she may be acting.

xviii. The client is publicly known to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds or is known to associate with such persons. Sources for this information include news items or internet searches.

xix. The client enquiries as to how quickly he or she can liquidate accounts or earnings without explaining why or provides suspicious reasons for doing so.

xx. The client opens an account or purchases a product without any regard to loss, commissions or other costs associated with that account or product.

xxi. The client has commercial or other types of relationships with risky persons or institutions.

xxii. The client acts through intermediaries, such as money managers or advisers, in order not to have his or her identity registered.

xxiii. The client exhibits unusual concern with the securities firm's compliance with government reporting requirements and/or the firm's AML/CFT policies.

xxiv. The client is reluctant to provide the securities firm with information needed to file reports or fails to proceed with a transaction once asked for documentation or learns of any recordkeeping requirements.

xxv. The client is interested in paying higher charges to the securities firm in order to keep some of his or her information secret.

xxvi. The client tries to persuade an employee of the securities firm not to file a required report or not to maintain required records.

xxvii. The client funds deposits, withdraws or purchases financial or monetary instruments below a threshold amount in order to avoid any reporting or recordkeeping requirements imposed by the jurisdiction.

xxviii. The client requests that account openings and closings in his or her name or in the name of family members be done without producing a paper trail.

xxix. Law enforcement has issued subpoenas regarding a client and/or account at the securities firm.

Funds Transfers and Deposits

i. Wire transfers are sent to, or originate from, financial secrecy havens, tax shelters or high-risk geographic locations (e.g. jurisdictions known to produce narcotics/psychotropic drugs or to be related to terrorism) without an apparent business reason or connection to a securities transaction.

ii. Wire transfers or payments to or from unrelated third parties (foreign or domestic) or where the name or account number of the beneficiary or remitter has not been supplied.

iii. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

iv. Many small, incoming wire transfers or deposits are made, either by the client or third parties, using cheques, money orders or cash that are almost immediately withdrawn or wired out in a manner inconsistent with the client's business or history.

v. Multiple personal and business accounts or the accounts of nonprofit organisations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

vi. Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.

vii. Incoming payments made by third-party cheques or cheques with multiple endorsements.

viii. Deposit of large amount of small-denomination currency to fund account or exchanges of small notes for bigger notes.

ix. Wire transfer activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

x. The securities account is used for payments or outgoing wire transfers with little or no securities activities (e.g. account appears to be used as a depository account or a conduit for transfers).

xi. The controlling owner or officer of a public company transfers funds into his personal account or into the account of a private company that he or she owns or that is listed as an authorised signatory.
xii. Quick withdrawal of funds after a very short period in the account.
xiii. Transfer of funds to financial or banking institutions other than those from where the funds were initially directed, specifically when different countries are involved.
xiv. Transfers/journals between different accounts owned by the client with no apparent business purpose.
xv. Client requests that certain payments be routed through correspondent accounts held by the financial intermediary or sundry accounts instead of its own account.

Unusual Securities Transactions and Account Activity

i. Transaction when one party purchases securities at a high price and then sells them at a considerable loss to another party. This may be indicative of transferring value from one party to another.
ii. A client's transactions include a pattern of sustained losses. This may be indicative of transferring value from one party to another.
iii. The purchase and sale of non-listed securities with a large price differential within a short period of time. This may be indicative of transferring value from one party to another.
iv. Payments effected by administrators and asset managers in cash, bearer cheques or other transferable instruments without identifying who they are for or providing very little information regarding the underlying account holder or beneficiary.
v. A company uses cash to pay dividends to investors.
vi. Use of shell companies to purchase public company shares, in particular if the public company is involved in a cash intensive business.
vii. Transfer of assets without a corresponding movement of funds, such as through journaling or effecting a change in beneficial ownership.
viii. A dormant account that suddenly becomes active without a plausible explanation (e.g. large cash deposits that are suddenly wired out).
ix. A client's transactions have no apparent economic purpose.
x. A client who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless.
xi. Transactions that show the client is acting on behalf of third parties.

xii. The purchase of long-term investments followed by a liquidation of the accounts shortly thereafter, regardless of fees or penalties.
xiii. Transactions involving an unknown counterparty.
xiv. Large sum cash purchases of financial instruments and mutual funds holdings followed by instant redemption.

Insurance Products (applicable to insurance products that can be considered as securities or having a securities related component in its structure)

i. The client cancels an insurance contract and directs that the funds be sent to a third- party.
ii. The client deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of the funds.
iii. The client cancels an annuity product within the free-look period. Although this could be legitimate, it could also signal a method of laundering funds if accompanied with other suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders and/or having a history of cancelling annuity products during the free look period.
iv. The client opens and closes accounts with an insurance company only to reopen a new account shortly thereafter with the same insurance company, but with new ownership information.
v. The client purchases an insurance product with no concern for investment objective or performance.
vi. The client purchases an insurance product with unknown or unverifiable sources of funds, such as cash, official cheques or sequentially numbered money orders.
vii. Securing a policy loan against the cash value soon after the policy is issued and repaying the loan with various monetary instruments or cash.
viii. Activity that is Inconsistent with the client's Business Objective or Profile
ix. The client's transaction patterns suddenly change in a manner that is inconsistent with the client's normal activities or inconsistent with the client's profile.
x. There are unusual transfers of funds or journaling (i.e. book entries) among accounts without any apparent business purpose or among apparently unrelated accounts.
xi. The client maintains multiple accounts or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
xii. The client's account is not used for its intended purpose (i.e. used as a depository account).

xiii. The client enters into a financial commitment that appears beyond his or her means.
xiv. The client begins to use cash extensively.
xv. The client engaged in extremely complex transactions where his or her profile would indicate otherwise.
xvi. Client's credit usage is in extreme amounts that do not correspond to his or her financial status or collateral, which is provided by an unrelated third-party.
xvii. The time zone in client's location is not consistent with the times that the trades were executed, with no apparent business or other purpose, or there is a sudden change inconsistent with the client's typical business activity.
xviii. A foreign based client that uses domestic accounts to trade on foreign exchanges.
xix. The client exhibits a lack of concern about higher than normal transaction costs.

Activity that is Inconsistent with the Client's Business Objective or Profile

i. The client's transaction patterns suddenly change in a manner that is inconsistent with the client's normal activities or inconsistent with the client's profile.
ii. There are unusual transfers of funds or journaling (i.e. book entries) among accounts without any apparent business purpose or among apparently unrelated accounts.
iii. The client maintains multiple accounts or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
iv. The client's account is not used for its intended purpose (i.e. used as a depository account).
v. The client enters into a financial commitment that appears beyond his or her means.
vi. The client begins to use cash extensively.
vii. The client engaged in extremely complex transactions where his or her profile would indicate otherwise.
viii. Client's credit usage is in extreme amounts that do not correspond to his or her financial status or collateral, which is provided by an unrelated third-party.
ix. The time zone in client's location is not consistent with the times that the trades were executed, with no apparent business or other purpose, or there is a sudden change inconsistent with the client's typical business activity.
x. A foreign based client that uses domestic accounts to trade on foreign exchanges.
xi. The client exhibits a lack of concern about higher than normal transaction costs.

Rogue Employees

i. The employee appears to be enjoying a lavish lifestyle that is inconsistent with his or her salary or position.
ii. The employee is reluctant to take annual leave.
iii. The employee is subject to intense job-related demands, such as sales or production goals that may make him more willing to engage in or overlook behaviour that poses ML/TF/PF risks.
iv. The employee inputs a high level of activity into one client account even though the client's account is relatively unimportant to the organisation.
v. The employee is known to be experiencing a difficult personal situation, financial or other.
vi. The employee has the authority to arrange and process client affairs without supervision or involvement of colleagues.
vii. The management/reporting structure of the financial institution allows an employee to have a large amount of autonomy without direct control over his activities.
viii. The employee is located in a different country to his direct line of management, and supervision is only carried out remotely.
ix. The management culture within the financial institution focuses on financial reward over compliance with regulatory requirements.
x. The employee's supporting documentation for clients' accounts or orders is incomplete or missing.
xi. Business is experiencing a period of high staff turnover or is going through significant structural changes.

Insider Trading

i. The client makes a large purchase or sale of a security, or option on a security, shortly before news is issued that affects the price of the security.
ii. The client is known to have friends or family who work for the securities issuer.
iii. A client's trading patterns suggest that he or she may have inside information.

Market Manipulation, including Penny Stocks

i. A client engages in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low-priced securities.
ii. Securities or funds transfers between parties without an apparent relationship.
iii. Securities transactions occur across many jurisdictions, and in particular high-risk jurisdictions.
iv. Two or more unrelated accounts at the securities firm trade an illiquid or low-priced security suddenly and simultaneously.
v. A client journals securities between unrelated accounts for no apparent business reason.
vi. A client has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
vii. Transactions between the same or related parties structured solely so that one side incurs a loss while the other incurs a gain.
viii. Transaction when one party purchases securities at a high price and then sells them at a considerable loss to another party.
ix. The client deposits a large number of physical securities at the securities firm.
x. The physical securities are titled differently to the name on the account.
xi. The physical security does not bear a restrictive legend even though the history of the stock and/or the volume of shares being traded suggest that it should have such a legend.
xii. The client's explanation regarding the method of acquiring the physical securities does not make sense or changes.
xiii. The client deposits physical securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
xiv. Large or repeated trading in securities that are illiquid, low priced or difficult to price.
xv. The company at issue has no apparent business, revenues or products.
xvi. The company at issue has experienced frequent or continuous changes in its business structure and/or undergoes frequent material changes in business strategy or its line of business.
xvii. The officers or insiders of the company at issue are associated with other low priced, illiquid or low volume companies.
xviii. The officers or insiders of the low priced, illiquid or low volume company have a history of regulatory violations.

xix. The low priced, illiquid or low volume company at issue has failed to make required regulatory disclosures.

xx. The low priced, illiquid or low volume company at issue has been the subject of a prior trading suspension.

xxi. A client's transactions include a pattern of receiving physical securities or receiving incoming shares transfers that are sold with the proceeds wire transferred out of the account.

xxii. The purchase and sale of non-listed securities with a large price differential within a short period of time.

APPENDIX III

INDICATORS OF TERRORIST FINANCING

FINTRAC (Financial Transactions and Reports Analysis Centre of Canada) noted that a single indicator on its own may seem insignificant, but combined with others, could provider reasonable grounds to suspect that the transaction is related to terrorist financing activity.

i. Client accesses accounts, and/or uses debit or credit cards in high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organisations.
ii. Client identified by media or law enforcement as having travelled, attempted/intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organisations.
iii. Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organisations.
iv. The client mentions that they will be travelling to, are currently in, or have returned from, a high-risk jurisdiction (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organisations.
v. Client depletes account(s) by way of cash withdrawal.
vi. Client or account activity indicates the sale of personal property/possessions.
vii. Individual/Entity's online presence supports violent extremism or radicalization.
viii. Client indicates planned cease date to account activity.
ix. Client utters threats of violence that could be of concern to National Security/Public Safety.
x. Sudden settlement of debt(s) or payments of debts by unrelated 3rd party(ies).
xi. Law enforcement indicates to reporting entity that the individual/entity may be relevant to a law enforcement and/or national security investigation.

xii. Client's transactions involve individual(s)/entity(ies) identified by media or law enforcement as the subject of a terrorist financing or national security investigation.

xiii. Client donates to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, NGO, etc.).

xiv. Client conducts uncharacteristic purchases (e.g. camping/outdoor equipment, weapons, ammonium nitrate, hydrogen peroxide, acetone, propane, etc.).

xv. A large number of email transfers between client and unrelated 3rd party(ies).

xvi. The client provides multiple variations of name, address, phone number or additional identifiers.

xvii. The sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.

xviii. Raising donations in an unofficial or unregistered manner.

xix. The use of funds by a non-profit organisation that is inconsistent with the purpose for which it was established.

APPENDIX IV

Examples of Enhanced Due Diligence (EDD) measures

Examples of EDD measures that could be applied for high-risk business relationships in the Securities Sector include, but are not limited to, taking more intrusive and exhaustive steps to:

i. Increase the quantity of information obtained for CDD purposes (e.g. request additional information to support the client's residential status, employment, salary details and other sources of income) and requesting additional documentary evidence or sourcing same through publicly available sources (e.g. scrutiny of negative media news, internet searches, use of social media).

ii. Further understand the client's ownership and control structure to ensure that the risk associated with the relationship is well-known. This may include obtaining and assessing information regarding the client's reputation, including any negative media allegations against the client.

iii. Further understand the intended nature of the business relationship and the reasons for intended or performed transactions. It may be appropriate to request a client's business plans, cash flow projections, copies of contracts with vendors, etc. The Registrant should understand why the client is requesting a certain service or product and particularly when it is unclear why a client is seeking to establish business relationships in another jurisdiction from where he is not domiciled. The account may have to be monitored for a period of time to establish a full view of the nature of activity and whether it fits with the initial risk profile of the client.

iv. Verify the source of funds, source of wealth of the client and/or volume of assets. Intrusive measures to verify the source of funds and wealth may be the only adequate risk mitigation measure. Possible sources may be reference to VAT and income tax returns, additional pay-slips, title deeds or, if from an inheritance, request a copy of the will and approved grant or documentation to evidence divorce settlement or sale of property or other assets.

v. Evaluate the principals and conduct reference checks and checks of electronic databases;

vi. Require that the first funds used to establish the investment relationship does not come from the account of a third party and comes from an account in the client's name held at a bank which is subject to similar CDD standards;

vii. Review current financial statements of the institutional client to, *inter alia,* verify source of funds, the institutional client's ability to generate income and the legitimacy of the client's operations; and

viii. Conduct enhanced, ongoing monitoring of the business relationship, by increasing the number and timing of controls applied, and through more frequent formal review.

APPENDIX V

Examples of Simplified Due Diligence (SDD) measures

i. The SDD measures outlined below are for guidance only and should not be considered as prescriptive or exhaustive. Where a Registrant determines, based on their risk assessment, that the ML/TF/PF risks are lower, the Registrant may apply one or more of the following SDD measures:

ii. Adjust the timing of CDD where the product or transaction has features that limit its use for ML/TF/PF purposes. Registrants may verify the client's or beneficial owner's identity after the establishment of the business relationship where the products or services provided have limited functionality or restricted services to certain types of client;

iii. Adjust the quantity of information requested from the client for identification, verification or monitoring purposes;

iv. Adjust the quality or source of information obtained for identification, verification or monitoring purposes. Where the risk associated with all aspects of the relationship is very low, Registrants may rely on the source of funds to meet some of the CDD requirements, for example, the purpose and intended nature of the relationship may be inferred where the sole inflow of funds are government pension or benefit payments; and

v. Adjust the frequency and intensity of transaction monitoring, for example, by monitoring transactions above a certain threshold only.

APPENDIX VI

Key components of the sanctions screening process

1. Utilization of sanctioned entity lists

Reporting Entities are legally required to screen customers and transactions against official sanctions lists. The FIUTT provides a specific **Targeted Financial Sanctions (TFS) Search Tool** that combines data from:

- The United Nations Security Council (UNSC) Consolidated List.
- The FIUTT's own Consolidated List of High Court Orders for designated entities in Trinidad and Tobago.

2. Risk-based approach

Reporting Entities must develop and maintain a risk-based compliance program to manage potential money laundering, terrorism financing, and proliferation financing (ML/FT/PF) risks. The screening process should consider risk factors related to customers, products and services, and geographic location. Higher-risk customers, such as Politically Exposed Persons (PEPs) or those from high-risk jurisdictions, may require enhanced due diligence (EDD) and more frequent screening.

3. Screening of customers and transactions

Sanctions screening is an integral part of the Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) processes.

- **Customer screening:** Screening should occur when establishing a business relationship and as part of ongoing monitoring. Periodic reviews help ensure that policies and procedures are appropriate and valid.
- **Transaction screening:** Individual transactions must also be screened to identify potential links to sanctioned entities. A higher-risk transaction may trigger a manual review.

4. Handling of a match

If a sanctioned individual or entity attempts to engage in a transaction or business relationship, the Reporting Entity must adhere to strict protocols:

- **Immediate freezing:** The institution must not enter into or continue any business transaction or relationship with the person or entity. All funds and assets must be frozen immediately.
- **Prompt reporting:** The Reporting Entity must file a **Suspicious Transaction Report (STR)** or **Suspicious Activity Report (SAR)** with the FIUTT without delay. The FIUTT provides an online submission process for these reports.

- **No "tipping off":** Staff must maintain confidentiality and avoid informing the customer that they have been flagged for sanctions screening.

5. Record-keeping and reporting

In addition to ad-hoc STR/SAR reporting, Reporting Entities must file quarterly reports with the FIUTT regarding designated terrorist property.

- **Quarterly Terrorist Property Report (QTR) 1:** Filed by entities that do not hold or control any terrorist property.
- **QTR 2:** Filed by entities that do hold or control terrorist property, including particulars of the accounts, persons, and value.

6. Training and compliance

Effective sanctions screening relies on well-trained staff and a strong culture of compliance.

- **Staff training:** Employees must receive regular, role-specific training on their AML/CFT obligations and procedures for identifying suspicious activities.
- **Independent audits:** Compliance programs must undergo independent audits and control testing to assess their effectiveness and identify any gaps.

Legal and regulatory framework

The operational protocols are underpinned by several pieces of legislation and regulations:

- **Anti-Terrorism Act (ATA):** Criminalizes terrorism financing and outlines prohibitions on transactions with listed entities.
- **Proceeds of Crime Act (POCA):** Requires Reporting Entities to submit STRs/SARs for suspected money laundering or terrorism financing.
- **Economic Sanctions Act:** Pertains to entities sanctioned under UN resolutions and requires Reporting Entities to take measures against them.
- **Guidance Notes from FIUTT:** The FIUTT issues official guidance notes and email notifications to Compliance Officers to provide detailed instructions on sanctions screening obligations and updates to sanctioned lists.