B

TRINIDAD AND TOBAGO SECURITIES AND EXCHANGE COMMISSION

Anti-Money Laundering and Counter Financing of Terrorism Guidelines for the Securities Sector

September 2018

Contents

SCOPE AND FOREWORD

The Trinidad and Tobago Securities and Exchange Commission (TTSEC) is governed by the Securities Act, Chap. 83:02 (SA 2012) which provides protection to investors from unfair, improper or fraudulent practices; fosters fair and efficient securities markets and confidence in the securities industry in Trinidad and Tobago; to reduce systemic risk. TTSEC is the designated authority for registering and regulating reporting issuers, self-regulatory organizations and Registrants to ensure their compliance with the provisions of the SA 2012 and other pertinent laws and regulations. To facilitate this function, section 6 of the SA 2012 establishes the functions of the TTSEC.

The Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT) framework of Trinidad and Tobago is spearheaded by the National Anti-Money Laundering Committee of Trinidad and Tobago (NAMLC) which is a multi-sectorial group made up of a number of key stakeholders.
The NAMLC was established to ensure that the relevant agencies including Supervisory Authorities/Regulators, Law Enforcement, Prosecutions and the Attorney General's Office develop sound AML/CFT policies and procedures to be used within their various sectors.

NAMLC has developed and implemented robust AML/CFT measures to effectively prevent and combat Money Laundering/Terrorist Financing (ML/TF). These measures include, inter alia, the adoption of the national AML/CFT suite of legislation.

To this end, in 2010 the Proceeds of Crime Act (POCA) specifically named the TTSEC as a Supervisory Authority (SA) for AML/CFT along with the Central Bank of Trinidad and Tobago (CBTT) and the Financial Intelligence Unit of Trinidad and Tobago (FIU). As an SA, the TTSEC is required to ensure that the financial institutions that it regulates comply with the AML/CFT legislation and implement robust AML/CFT frameworks that are commensurate with their size, complexity and risk profile. The TTSEC has developed a risk-based approach to inspecting its Registrants and has applied risk ratings accordingly.

To ensure such compliance the TTSEC has the power to issue Compliance Directions and to apply such other enforcement actions to address issues of non-compliance with those Directions.
The TTSEC also applies a collaborative approach to AML/CFT regulation and has entered into written agreements and Memoranda of Understanding (MoUs) to ensure the exchange of information with local and foreign authorities, where applicable.

Notwithstanding the collaborative approach, the TTSEC's AML/CFT risk methodology and approach to AML/CFT regulation takes into account specific issues unique to its Registrants.
Accordingly, these Guidelines outline the TTSEC's framework for the supervision and enforcement of the national AML/CFT suite of legislation with a view to mitigating ML/TF risks in the securities sector.

These Guidelines replace the TTSEC AML/CFT Guidelines issued in November, 2011 and seek to better inform the TTSEC's Registrants of their need to implement effective policies and procedures to comply with the national AML/CFT legislative framework.

The TTSEC notes that some of its Registrants are dually registered with the Central Bank of Trinidad and Tobago (CBTT). Notwithstanding this, dually registered entities are required to comply with these Guidelines when engaging in the activities for which they are registered under the Securities Act Chap. 83:01.

MONEY LAUNDERING AND THE FINANCING OF TERRORISM

The goal of most, if not all, criminal activity is to generate a profit for those who commit the criminal acts. Money laundering is the process used to disguise the illicit source of the profit, i.e. money or assets, derived from criminal activity.

There are three stages of money laundering:

1. 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;

2. 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;

3. 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.

While the securities sector (with the exception of 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 the 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.

Unlike money laundering, terrorism financing is not usually committed with the goal of making a profit. Terrorism is the unlawful threat of action designed to compel the government or an international organization or intimidate the public or a section of the public for the purpose of advancing a political, religious or ideological belief or cause. Financing of terrorism (FT/TF) is the process by which funds are provided to an individual or group to finance 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 organizational costs to develop and maintain an infrastructure of organizational support and to promote the ideology of a terrorist organization.

Also unlike money laundering, 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.

THE ROLE OF TTSEC AS THE SUPERVISORY AUTHORITY

The POCA, the Financial Obligations Regulations (FOR) and the Anti-Terrorism Act, Chap. 12:07 (ATA) designate the TTSEC as the AML/CFT SA for the following financial institutions:

- Broker-Dealers;
- Investment Advisers; and
- Underwriters.

TTSEC employs the following approaches, among others, to carry out its AML/CFT supervisory functions:

- Issuance of AML/CFT Guidelines. These Guidelines outline the minimum requirements of Registrants in fulfilling their AML/CFT obligations. The Guidelines will be updated where it becomes necessary based on changes in the national AML/CFT framework;
- Conducting On-Site and Off-Site Inspections to determine the Registrant's implementation of the requirements under the relevant AML/CFT legislation and/or relevant Guidelines issued by the TTSEC;
- Conducting Sectorial Risk Assessments;
- Conducting Market Entry Surveillance;
- Approval of Compliance Officers (CO) and Alternate Compliance Officers (ACO);
- Taking proportionate and dissuasive regulatory action against those regulated financial institutions and persons which fail to comply adequately with AML/CFT statutory obligations and Guidelines issued by TTSEC;
- Sharing information with the FIU, Central Bank and other regulatory agencies as required for the purposes of AML/CFT. This includes disclosing information to the FIU as soon as is reasonably practicable where it has knowledge or has reasonable grounds for believing that a financial institution may have been engaged in money laundering or terrorist financing; and
- Conducting market outreach meetings with its Registrants

COMPLIANCE WITH THESE GUIDELINES

(A) All Registrants must comply with the requirements of these AML/CFT Guidelines within six (6) months of the issuance of these AML/CFT Guidelines.

(B) Registrants will be required to conduct their 2019 AML/CFT external audits using this revised AML/CFT Guideline. TTSEC recognizes that in some instances, Registrants would not have completed their implementation plan by the 2019 audit cycle, however in such instances; the external audit should consider the status of the financial institution's implementation plan in its assessment.

(C)Failure to comply with these Guidelines after the said transitional period may result in action being taken by the Commission in keeping with its powers under the Securities Act 2012.

LIST OF ACRONYMS & ABBREVIATIONS

ACO	Alternate Compliance Officer
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (also used for Combating the financing of terrorism)
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
FIU	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
FOR	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	Supervisory Authority
SA 2012	Securities Act, Chap. 83:02
SDD	Simplified Due Diligence
TTSEC	Trinidad and Tobago Securities and Exchange Commission

LEGISLATIVE FRAMEWORK

The AML/CFT legislative framework of Trinidad and Tobago comprise the following key laws:

• Proceeds of Crime Act and Regulations, Chapter 11:27;

• The Anti-Terrorism Act and Regulations, Chapter 12:07; and

• The Financial Intelligence Unit of Trinidad and Tobago Act and Regulations, Chapter 72:01.

TTSEC'S AML/CFT GUIDELINES FOR THE SECURITIES SECTOR

1. These Guidelines are being issued pursuant to Section 146 of the SA 2012 and Regulation 40A of the FOR and is intended to assist Registrants with, inter alia, complying with Trinidad and Tobago's AML/CFT laws including applying a risk-based AML/CFT approach through:

   (a) Understanding and complying with AML/CFT legislative and regulatory requirements;

   (b) Developing and implementing effective, risk-based AML/CFT 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 controls.

2. From time to time TTSEC will amend this Guideline to address changes in the AML/CFT legislative framework. However, Registrants should, as part of their risk management practices, stay current with emerging developments as they relate to AML/CFT and update their AML/CFT programs as necessary.

PART 1: INTERPRETATION OF THE AML/CFT GUIDELINES

3. In these Guidelines, unless otherwise stated –

"AML/CFT Guidelines" refers to these Guidelines

"beneficial owner" means –

(a) the person who ultimately owns and controls an account, or who exercises ultimate control over a legal person or legal arrangement, or the natural person on whose behalf a transaction is being conducted; and

(b) in relation to a security, means a person who has beneficial ownership of the security although that person may not be the registered owner of the security;

“beneficial ownership” includes –

(a) ownership through a trustee, legal representative, agent or other market actor;

(b) in relation to a security, entitlement to the benefits of ownership of the security and includes direct ownership, ownership through a trustee, legal representative, agent or other intermediary, and a person shall be deemed to have beneficial ownership of a security, including an unissued security, if the person is the beneficial owner of a security or securities convertible into the underlying security—

(i) under all circumstances; or

(ii) by reason of the occurrence of an event that has occurred and is continuing;

“Board of Directors” or “Board” means the body or person responsible for overseeing the performance of the Registrant;

“Broker-Dealer” means a person engaging in, or holding himself out as engaging in, the business of —

(a) effecting transactions in securities for the account of others;

(b) buying or selling securities for his own account and who holds himself out at all normal times, as willing to buy and sell securities at prices specified by him; or

(c) such other activities as may be prescribed.

“Entity” means a body corporate, trust, partnership, collective investment scheme, fund or other unincorporated enterprises or organizations;

“Financial Intelligence Unit” means the Financial Intelligence Unit established under section 3 of the Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01;

“foreign client” means a person who resides outside of Trinidad & Tobago at the time of onboarding and who continues to reside outside of Trinidad & Tobago throughout the business relationship;

“freezing order” refers to an Order of the Court obtained by the Attorney General under Section 22B of the Anti-Terrorism Act, Chapter 12:07;

“institutional client” refers to all clients that are not retail clients;

“investment advice” means advice with respect to an investment in, or the purchase, sale or holding of, a security;

“investment adviser” means a person engaging in, or holding himself out as engaging in, the business of providing investment advice, and includes a person that provides investment advice to a manager of a collective investment scheme;

“Legal persons” refer to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

“One-off transaction” means any transaction other than one carried out in the course of an existing business relationship;

“Non-Profit Organisation” has the meaning assigned to it in the Anti-Terrorism Act, Chap. 12:07;

“politically exposed person” means—

(a) individuals such as the Head of State or Government, senior politician, senior government, judicial or military officials, senior executives of State-owned corporations and important political party officials who are or have been entrusted with prominent functions–

(i) by a foreign country; or

(ii) domestically for Trinidad and Tobago;

(b) persons who are or have been entrusted with a prominent function by an international organization which refers to members of senior management such as directors and members of the board or equivalent functions;

(c) an immediate family member of a person referred to in paragraph (a) such as the spouse, parent, siblings, children and children of the spouse of that person; and

(d) any individual publicly known or actually known to the relevant financial institution to be a close personal or professional associate of the persons referred to in paragraphs (a) and (b);

“Registrant” means:

(a) Broker-Dealers;

(b) Investment Advisers; and

(c) Underwriters

“retail client” means a natural person who is a client of, or is seeking to establish a business relationship with, a Registrant;

“security” has the meaning assigned to it in the SA 2012;

“senior management” means the managing director, the chief executive officer, chief operating officer, the deputy managing director, the president, the vice-president, the secretary, the treasurer, the chief financial officer, the financial controller, the general manager, the deputy general manager, corporate secretary, chief accountant, chief auditor, chief investment officer, chief compliance officer and chief risk officer of an entity or any other individual who performs functions for an entity similar to those normally performed by an individual occupying any such office;

“underwriter” has the meaning as assigned to it in the SA 2012.

PART 2: INTERNAL POLICIES AND PROCEDURES

Risk-Based Approach

4. (1) The FATF Report on Money Laundering and Terrorist Financing in the Securities Sector (October 2009) outlines the main ML/TF vulnerabilities in the securities sector. Some of the key characteristics of the securities sector which makes it more vulnerable to ML/TF abuse are as set out at Appendix 1 of these Guidelines. The nature and complexity of the securities sector means that the risks encountered by Registrants may differ from the risks encountered by other financial institutions who operate in financial sectors external to the securities sector. Therefore, Registrants must implement measures that are commensurate with their assessed risks.

(2) All Registrants are, therefore, required to utilize a risk-based approach[1] in the performance of all of its AML/CFT responsibilities.

(3) In applying a risk-based approach, each Registrant must ensure that it implements processes which enable it to:

(a) Identify the ML and TF risks which are specific to the Registrant itself and to its clients;
(b) Assess the risks identified and apply an appropriate risk rating;
(c) Monitor the risks identified in a manner which is proportionate to the risk rating; and
(d) Manage the risks identified with a view to mitigating such risks to the Registrant's best ability.

(4) In pursuance of Guideline 4(4), each Registrant must develop and implement a documented and Board approved risk assessment and rating policy which assesses the risk of, at a minimum, the Registrant's:

(a) Country/geographic location;

[1] Further guidance on a risk based approach can be found in FATF's paper entitled GUIDANCE FOR a RISK-BASED APPROACH - SECURITIES SECTOR, October 2018.

(b) Products and/or services: Factors a Registrant may consider in assigning risk scores would be ease of convertibility of the product to cash, ease of change of ownership, length of time before the investment product matures, percentage of foreign ownership of the product, internationally traded products etc.;
(c) Customers: Factors a Registrant may consider in assigning risk scores would include customer type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size and volume of transactions, type of transactions, cash transactions, etc.;
(d) Transaction types; and
(e) Delivery channels: such as the use of on-line services and wire transfer services.

(5) Registrants are required to have policies, controls and procedures 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.

(6) 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 commensurate with the risks identified pursuant to Guideline 4(4) and documented in the AML/CFT compliance programme.

(7) 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 legislation and these AML/CFT Guidelines.

(8) The risk assessment and rating policy should also contain processes for the following:
(a) Clearly documenting all AML/CFT risk assessments;
(b) Approving any change to risk ratings;
(c) Applying SDD, CDD and/or EDD measures in accordance with the assigned risks;

(d) Recording reasons for not complying with the organizations risk mitigation policies, procedures and controls contained in the risk assessment and rating policy;

(e) Providing the risk assessments and details of SDD, CDD and EDD processes to TTSEC if and when requested; and

(f) Assessing high risk clients more frequently than other clients. 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.

(9) When deciding to discontinue a business relationship, the Registrant should give consideration to whether or not a Suspicious Activity Report should be made to the FIU and whether terminating the relationship would tip off the client.

(10) Registrants should ensure that any changes to the risk ratings of clients are documented and the reasons for the changes clearly outlined.

(11) Registrants should take into account the following non-exhaustive risk criteria when determining the 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 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) The existence of any delegated form of authority such as but not exclusive to a power of attorney;
(j) The product or service utilized by the client;
(k) 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;
(l) Whether the account/business relationship is dormant; and
(m) Any other information that raises suspicion of the client being connected to ML or TF activities.

(12) A Registrant must identify and assess the ML/TF risks that may arise in the 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.

(13) A Registrant must in respect of new products and new business practices:
(a) Undertake the risk assessments prior to the launch or use of such products, practice and technologies; and
(b) Take appropriate measures to manage and mitigate risks.

Compliance Programme

5. (1) Each Registrant must develop and implement a written AML/CFT compliance programme, approved by the Registrant's Board of Directors and reasonably designed to ensure compliance with the AML/CFT suite of legislation. Please refer to Appendix 2 for additional guidance regarding the role of the Board's oversight responsibilities.

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

(3) Regulation 7(4) of the FOR identifies measures, to which Registrants are required to adhere, for the application of Group-wide AML/CFT compliance programmes including:

(a) Policies and procedures for information sharing within the group for the purposes of CDD and ML/TF risk management;
(b) The provision, at group level compliance, audit and AML/CFT functions of client, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and
(c) Adequate safeguards for confidentiality and use of information exchanged.

(4) An AML/CFT compliance programme referred to in regulation 7(1) of the FOR must be based on the Registrant's risk assessment and rating policy and must at a minimum include—

(a) a system of internal controls to ensure ongoing compliance;
(b) internal and external independent testing for compliance;
(c) training of personnel in the identification of suspicious transactions; and
(d) appointment of a staff member responsible for continual compliance with the POCA and the FOR.

(5) An AML/CFT compliance programme may be designed such that it contains supplemental policies and procedures, however, such policies and procedures should be incorporated into the AML/CFT compliance programme by explicit reference.

(6) A Registrant's written AML/CFT compliance programme must be made available to all new and existing employees and should be easily accessible for reference and training purposes.

(7) The Registrant's AML/CFT compliance programme should be reviewed periodically and updated in a timely manner.

Designation of a Compliance Officer

6. (1) A Registrant must designate a CO employed at a managerial level for the purpose of securing compliance with all AML/CFT laws and regulations and to address other related issues.

(2) A Registrant who is part of a financial group which utilizes a group-wide approach to AML/CFT compliance may choose to appoint a Group CO, however, the TTSEC must be immediately notified of the appointment in writing.

(3) Notwithstanding the appointment of the Group CO, each Registrant must designate its own CO who is employed by the Registrant, or employed within the same Financial Group as the Registrant provided that appropriate service level arrangements are in place. This CO must be employed at a managerial level.

(4) 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.

(5) 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 3 of the FOR. The senior employee need not be employed at a managerial level but must have the requisite authority to fulfil the functions of the CO as defined by regulation 4 of the FOR.

(6) 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.

(7) In the case of a Registrant who is an individual and does not employ or act in association with any other person, that Registrant need not appoint an ACO.

(8) Registrants must seek the approval of TTSEC for the appointment of its designated CO and the ACO.

(9) Applications for the approval of COs and ACOs should be made to TTSEC in the manner as prescribed by TTSEC and should be accompanied by all requested documents.

(10) Where a Registrant is also registered with the CBTT, the Registrant must submit applications for the approval of a CO simultaneously to each SA. The application to each SA should indicate that an application was also submitted to the other SA. The SAs 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.

(11) The TTSEC's prescribed application form for the approval of COs and ACOs can be found on the TTSEC's website.

(12) The identities of the CO and ACO must be treated with the strictest of confidence by the Registrant and all members of staff.

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

(14) Registrants should ensure that COs and ACOs receive the appropriate training so as to enable them to detect potential money laundering and terrorist financing activities and perform all other duties as set out in these AML/CFT Guidelines and the FOR.

Functions of the Compliance Officer

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

(a) Have oversight of the AML/CFT control activity in all relevant business areas for the purposes of establishing a reasonable threshold level of control consistency throughout the Registrant's business;

(b) Keep the AML/CFT compliance programme current relative to the Registrant's identified inherent risks with consideration given to local and international developments in ML and TF;

(c) Ensure regular risk assessments of the inherent ML and TF risks, including timely assessments of new products, services and business acquisition initiatives to identify potential ML/TF risks and develop appropriate control mechanisms, are conducted;

(d) Ensure periodic assessments of AML/CFT control mechanisms, to confirm their continued relevance and effectiveness in addressing changing ML/TF risks, assess operational changes, including the introduction of new technology and processes to ensure that ML/TF risks are addressed, are conducted;

(e) 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;

(f) Ensure the development of written AML/CFT policies and procedures are kept up to date and approved by the Board of Directors;

(g) Ensure that ongoing AML/CFT training programmes are carried out for all new and existing employees, senior management and the Board of Directors, on AML/CFT and ensure that such AML/CFT training programmes are up-to-date and relevant to the Registrant's business;

(h) 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;

(i) Report relevant information to the Board of Directors and/or senior management regarding the adequacy of the AML/CFT framework or any associated issues; and

(j) Ensure any changes to the AML/CFT compliance programme are disseminated to all employees and assist departments in the implementation of the AML/CFT compliance programme.

(2) The duties and responsibilities performed by the CO should be documented in the COs job description.

(3) For consistency and to ensure ongoing attention to the compliance regime, the appointed CO may delegate certain duties to other employees. However, where such a delegation occurs, the CO retains responsibility and accountability for the AML/CFT compliance programme.

(4) 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 organization.

Know Your Employee

8. (1) 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 of the existing or prospective employee.

(2) The due diligence measures include but are not limited to the following activities-

(a) verification of identity;

(b) verifying employment history, reference checks, checking authenticity of academic qualifications;

(c) checking criminal record of the staff member.

(3) 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.

(4) A Registrant should maintain a record of the names, addresses, position titles and other official information pertaining to staff members appointed or recruited by them for up to

period of six (6) years after the termination of employment and make available to TTSEC on request.

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

(6) The Registrant's written policies and procedures should include a code of ethics which must serve to guide all employees in the conduct of their duties.

(7) AML/CFT 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

9. (1) Registrants should establish ongoing AML/CFT training programmes for Directors, senior management and staff at all levels, both new and existing.

(2) Training should be held at least once annually.

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

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

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

(a) identify the risks associated with ML/TF, understand their ML/TF risk exposure specific to their job function and understand how the institution might be used for ML/TF;
(b) be aware of techniques and trends utilized in ML and TF;
(c) be aware of the legal penalties for non-compliance with these AML/CFT Guidelines and related legislation;
(d) be aware of processes for detecting ML or TF 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;

(6) New employees should undergo an initiation in AML/CFT generally and specific to their role in the Registrant's business.

(7) 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.

(8) The Registrant should keep a written record of compliance with (1) and (2) above.

Internal and External Audit

10. (1) A Registrant must have their AML/CFT compliance programme reviewed on a regular basis by both internal and external auditors.

(2) External Audits should be conducted on an annual basis in keeping with Regulation 10(2)(a) of the FOR.

(3) The frequency of internal audit review may be determined by the Registrant commensurate with its complexity, size and risk profile, but at a minimum should be conducted every three (3) years. Internal audits should be conducted in keeping with Regulation 10(2)(b) of the FOR.

(4) In the case of Registrants who are individuals, who neither employ nor acts in association with another person, an internal audit review will not be considered mandatory, however, such Registrants must conduct an external audit on an annual basis.

(5) Where a Registrant fails to engage the services of an auditor, either internal or external, TTSEC must appoint, a competent professional to carry out the functions listed hereunder with the cost to be borne by the Registrant.

(6) It is necessary that these reviews are performed by auditors who have had appropriate AML/CFT training and experience in respect of ML and TF risk relevant to the Registrant's business and an appropriate level of knowledge of the regulatory requirements and guidelines.

External Auditor

11. (1) The external auditors must submit their report in the approved ICATT format[2] to the TTSEC and the Board of Directors of the Registrant within four (4) months of the end of the Registrant's financial year.

(2) The audit report must be accompanied by the curriculum vitae of the person(s) who performed the audit, detailing their training and experience in AML/CFT and the conduct of compliance audits.

Internal Auditor

12. (1) The Internal Auditor must ensure that the Registrant's internal policies, procedures and systems are in compliance with the requirements of the FOR and that the level of transaction testing conducted is suitable to the risk profiles of the clients of the Registrant.

(2) The internal audit may include, inter alia:

[2] The Institute of Chartered Accountants of Trinidad and Tobago (ICATT) worked with the Central Bank, TTSEC and the FIU to agree a format for external audits reviews of financial institutions' AML/CFT compliance programme.

(a) A review of the Registrant's risk assessment and rating policy for reasonableness given its risk profile as set out in these Guidelines;

(b) Determining the adequacy of the Registrant's ML/TF risk assessment and rating policy and application of a risk-based approach in the design of its AML/CFT policies, procedures and controls;

   (c) Appropriate risk-based testing of client files and transactions to verify adherence to the AML/CFT 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 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. It should be noted that the internal audit review does not include a review of actual SAR/STRs filed with the FIU.

(3) The internal audit review may 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 legislative requirements and the Registrant's policies and procedures.

(4) The Internal Audit review process should identify weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions, including ensuring that recommendations made by the external auditor and the TTSEC have been satisfactorily addressed.

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

PART 3: CUSTOMER DUE DILIGENCE (CDD)

General CDD

13. CDD is an important protection for the Registrant against client who may misuse the Registrant for the purpose of Money Laundering and Terrorist Financing. It is a basic prudential principle that a Registrant should know the identity of the person that it is transacting business with and the purpose of the transaction. CDD applies to both retail and institutional clients.

14. (1) Registrants are required to conduct client due diligence including the verification of client identity in circumstances which include, but are not limited to, the following:
    - (a) Establishing a business relationship;
    - (b) For one-off transactions or occasional transactions of a value equivalent to TT$90,000 or more;
    - (c) For two or more one-off transactions which together total a value equivalent toTT$90,000 or more and which appear to be linked;
    - (d) For one-off wire transfers of a value equivalent to TT$6,000 or more; and
    - (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; or

(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 an STR with the FIU.

(2) 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.

(3) Any client's transaction which falls within the parameters identified above at Guidelines 14(1) (a) – (e)must be supported 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.

(4) Documentation to substantiate the source of funds may be used to support a series of transactions undertaken by a client. However, 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.

(5) Irrespective of the size of the transaction, any suspicious activity must be reported to the FIU.

15. 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. Please refer to Guideline 28 for further guidance on Ongoing Due Diligence.

Beneficial Ownership

16. (1) 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.

(2) 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.

(3) Reference to "ultimately own or control" refers to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. Registrants should take reasonable measures to look behind the legal entity to identify those who have ultimate control over the business and the legal entity's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the legal entity.

(4) 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.)

CDD for New and Existing Retail Clients

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

(2) 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' license.

(3) 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.

(4) A Registrant is prohibited from opening anonymous accounts or accounts in fictitious names. Where 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, or if it is already established, must immediately terminate the business relationship. In such a case, the Registrant should immediately file a SAR with the FIU.

(5) 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;
(b) Permanent address;
(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;
(h) Purpose of the proposed business relationship or transaction and source of funds;
(i) Any other information deemed appropriate by the Registrant.

(6) 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 16 and should obtain the relevant documentation which gives the client/applicant the legal authority to act for the beneficial owner (for example, powers of attorney, letters of authorization).

Verification of Identification

18. 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 the verification of identity in these exceptional circumstances.

Verification of Address

19. (1) 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) Checking the Register of Electors; or
    - (c) Documented record of a home visit.

(2) Electronic Bills or Paperless Bills are acceptable, however, Registrants must ensure that its 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.

(3) 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.

(4) 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 copy of contract of employment, or banker's or employer's written confirmation;

(5) 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;

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

Copies of Documents

20. Where original documents are not available, copies should be acceptable only where they are certified by identification. In the case of clients not present in Trinidad and Tobago, certification should be done by 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

21. The requirement to obtain documentary evidence of a client's place of business/occupation and 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

22. (1) Registrants must obtain the relevant documentation as outlined in Guideline 17, with appropriate adaptations, when onboarding companies, partnerships and sole traders. Examples of appropriate adaptations of Guideline 17 for companies would include the company name, registered address and country of incorporation.

    (2) Registrants should implement appropriate adaptations of Guideline 17 for self-employed clients who are not able to provide pay slips 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 a taxi badge, wireman's license or copies of lease agreements and rental receipts for landlords.

23. (1) 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).

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

24. (1) 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.

(2) If a prospective institutional client cannot provide the documentation stated at sub-Guideline 1(a) and (b) above, the Registrant may request other documentation to prove the source of funds to be used for the transaction (e.g. rental income earned by a landlord may be substantiated by lease agreements, deeds to verify ownership of property and bank statements showing earnings from rental; other self-employed individuals may produce relevant documentation to substantiate revenue streams including bank statements, invoices, receipts, contracts etc.).

(3) 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 into the business relationship (for example a copy of the Board Resolution authorizing the investment).

25. (1) Verification and update of identification documentation of the key functionaries of an institutional client should be conducted at least once annually by the Registrant for high risk clients.

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

(3) 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

26. Where the business relationship involves 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.

Trust Fiduciaries

27. (1) Where an applicant for business is a trustee, nominee or other legal arrangement, in addition to applying customer due diligence measures (with appropriate adaptations) outlined in Guideline 17, the Registrant must obtain the following:

    (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;
    (d) Verification of the identity of person(s) with the power to add beneficiaries (where applicable); and
    (e) Verification of the identity of the person providing funds if not the ultimate settlor.

(2) Verification of the identity of a beneficiary or other legal arrangement must be carried out before the pay-out or the exercise of any vested rights. The Registrant should undertake reasonable measures to verify the identity of the beneficial owners of the legal arrangement.

(3) 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 Grant of Probate, and/or 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.

(4) 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; and
(c) Accessing or searching public and private databases or other reliable independent sources.

(5) Registrants should verify that any person purporting to act on behalf of the legal arrangement is so authorized 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).

(6) 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 the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice.

(7) 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.

(8) 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) 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.

(10) 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 endeavour 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.

(11) There are a number of commercial structures in which a trust may feature as the legal owner, such as in debt repackaging arrangements. 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.

Ongoing Due Diligence

28. (1) 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 client's source of funds.

(2) 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 14(b) – (e) (whether one-off or not) throughout the business relationship.

(3) 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 FIU.

(4) 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.

Enhanced Due Diligence

29. (1) Where Registrants have identified higher risks of ML and/or TF 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 in order to determine whether the transactions and/or activities appear unusual or suspicious.

(2) 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.

30. EDD must also be applied in the following circumstances:
    (a) Clients with ties to countries which do not 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) When establishing counterparty business relationships (e.g. foreign Broker-Dealers, foreign custodians);
(d) Where the client is a foreign politically exposed person (PEP);
(e) Where higher risks have been identified with a client who is a domestic PEP or a PEP associated with an international organization;
(f) Non face-to-face business relationships or transactions; and
(g) in any other situation where money laundering risks are higher.

31. (1) 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.

(2) 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.

32. 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.

Examples of EDD measures

33. Examples of Enhanced Due Diligence 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:
(a) 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).

(b) 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.

(c) 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.

(d) 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.

(e) Evaluate the principals and conduct reference checks and checks of electronic databases;

(f) Requiring 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;

(g) 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

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

PEPs

34. (1) 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 and bribery, as well as conducting activity related to TF.

(2) Regulation 20 of the FOR defines who must be considered a PEP.

(3) 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.

(4) These requirements are intended to be preventive and should not be interpreted as stigmatising all PEPs as being involved in criminal activity. Some PEPs are neither in a position to, nor do they abuse their official position. 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 these AML/CFT Guidelines.

(5) Registrants must take reasonable measures to determine whether a client is a Foreign or domestic PEP.

Foreign PEPs

35. 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.

Domestic PEPs

36. If a client is a Domestic PEP or a director or member of the board (or equivalent function) of an international organization then:

    (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 known or actually known to the Registrant to be a close personal or professional associate of the client

    must only be subject to EDD measures where higher risks are identified.

37. 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 investigation or regulatory action.

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

    (a) ensure that approval is obtained from a 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 greater oversight of PEPs' accounts and EDD measures.

    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.

39. 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.

40. 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.

41. 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.

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

43. 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.

44. For additional guidance and information regarding PEPs, please see the FIU Guidance Note: AML/CFT Procedures for Politically Exposed Persons.

NPOs

45. FATF defines an NPO as “a legal person or arrangement or organization 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’.”

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

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

48. (1) 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.

    (2) In this regard, it is important for Registrants to determine the level of risk associated with the activities which the NPO engages in and make the appropriate distinction between those that serve a limited social or regional purpose from those whose activities and connections are more sophisticated, or are geographically based near to conflict zones and/or with financial links to other countries.

Considerations for assessing NPO risk

49. To assess the risk of an NPO, a Registrant should consider:

    (a) The evidence of registration under applicable laws of the home and local operation;
    (b) The purpose, ideology or philosophy of the NPO;
    (c) The geographic areas served (including headquarters and operational areas);
    (d) organizational 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.

50. 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.

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

52. 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 activities.

Simplified Due Diligence

53. Where a Registrant's risk assessment has identified lower ML/TF 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).

54. 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.

55. (1) 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.

(2) 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 FOR. 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.

(3) 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.

(4) 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.

56. 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.

57. 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.

Examples of SDD Measures

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

(a) Adjust the timing of CDD where the product or transaction has features that limit its use for ML/TF 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;

(b) Adjust the quantity of information requested from the client for identification, verification or monitoring purposes;

(c) 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;

(d) Adjust the frequency of CDD updates and reviews of the business relationship. This may be applied for example when trigger events occur such as the client requesting a new product or service or when a certain transaction threshold is reached. Registrants must ensure that this does not result in a de facto exemption from keeping CDD information up-to-date; and

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

(2) Where Registrants choose to use thresholds, 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.

Third Party Reliance

59. (1) There may be instances where a Registrant may rely on third party information to avoid duplication and additional costs. For example, when an investment adviser refers business to a broker-dealer or where a Registrant is on-boarding a client who has already been on-boarded within the financial group to which it belongs.

(2) In such cases, Registrants may rely on third party financial institutions for the 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 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.

(3) In such instances where third party reliance is used the ultimate responsibility and accountability remain with the Registrant that is placing reliance on the third party.

60. It is important to note that third party reliance is different from introduced business or an outsourcing arrangement. In a third party reliance scenario, the third party will typically have an existing relationship with the client that is independent of the relationship to be formed by the client with the relying financial institution.

61. The basis for deciding to place reliance on a third party for CDD must be documented and approved by senior management. The third party being relied on should not itself present higher ML/TF risk such as being located in a jurisdiction that has been identified as having strategic AML/CFT deficiencies.

62. 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.

63. At the minimum, financial institutions 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 the CDD information and provide copies of the relevant documentation immediately upon request; and
   (d) is properly regulated and supervised.

64. 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 manner as comprehensive as itself.

Information Sharing

65. (1) Where appropriate and practical and where there are no data protection restrictions, Registrants should take reasonable steps to ensure that where customer due diligence information is available in one part of the business, that there are information sharing mechanisms to link it to information held in another.

(2) 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.

(3) 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 other FSRBs.

66. 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.

Cross-Border Relationships

67. 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 management before establishing new counterparty relationships; and
    (d) Document the respective responsibilities of Registrant and the counterparty.

68. 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 is able to provide relevant CDD information upon request to the counterparty.

69. 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

70. The POCA and the FOR identify non face-to-face business relationships or transactions as high risk to which EDD must be applied.

71. 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.

72. (1) 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.

    (2) 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.

    (3) 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.

    (4) 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).

73. Registrants are reminded that they 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.

New Technologies

74. (1) Registrants should pay special attention to any money laundering and terrorist financing threats that may arise from new or developing products, new business practices including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

    (2) In particular, Registrants must undertake risk assessments prior to the launch or use of such products, practices and technologies; and should have policies and procedures in place to manage and mitigate the risks identified.

PART 4 – WIRE TRANSFERS

75. It is imperative that Registrants are aware of the ML/TF 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 compliance programme.

76. (1) While effecting wire transfers are under the remit of commercial banks, Registrants have an obligation to keep sufficient records to substantiate the originator, underlying client and beneficiary of the wire transmission.

    (2) These records should be kept in a format which enables it to be produced immediately to the FIU and to the TTSEC on request.

77. 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 information regarding the underlying client should also be included in the wire transmission.

78. (1) These Guidelines on wire transfers aim to ensure that 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

is immediately available:

(i) To Registrants to facilitate the identification and reporting of suspicious transactions;

(ii) To the FIU for analyzing suspicious activity and disseminating as necessary; and

(iii) 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.

(2) 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 effect 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

79. Domestic and Cross-border wire transfers should be accompanied by accurate and meaningful originator and beneficiary information. Wire transfers must always contain:

(a) The name of the originator and the underlying client on whose behalf the transfer is sent;

(b) The address or national identification number or a passport number of the originator and the underlying client;

(c) The account number of the originator, or in the absence of an account number, a unique transaction number which permits tracing of the transaction;

(d) The name of the beneficiary; and

(e) The beneficiary account number where that account is used to process the transactions, or in the absence of an account, a unique transaction number which permits tracing of the transaction.

PART 5: RECORD KEEPING REQUIREMENTS

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

Retention Period

81. Registrants must retain records of all domestic and international transactions and identification data obtained through the CDD process in either written or electronic form for a minimum period of six (6) years.

82. 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.

83. 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

84. (1) Notwithstanding Guideline 81 above, TTSEC or the FIU may extend the requirement of retaining records beyond the stipulated six (6) year period.

    (2) Where there has been a report of a suspicious activity via a SAR or where there is an ongoing investigation by the FIU 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 FIU or a Court of competent jurisdiction that it is safe to dispose of these records.

85. (1) 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 FIU.

    (2) These records should contain sufficient detail to permit the reconstruction of a specific transaction.

Requirement to make records available

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

87. Records should contain the following data as outlined in Regulation 32(1) of the FOR-
    - (a) Details of the transaction including the amount and type of the currency used, account files and business correspondences; and
    - (b) A copy of any documentation utilized in the CDD process.

PART 6: SUSPICIOUS ACTIVITY REPORTING

88. If a Registrant suspects or has reasonable grounds to suspect that client's funds are the proceeds of criminal activity or are related to terrorist financing, the Registrant must file a Suspicious Activity Report with the FIU as soon as possible, but in any event, within fourteen (14) days of the date on which the Registrant determined suspicion or had reasonable grounds to suspect that the client's funds are the proceeds of criminal activity or are related to terrorist financing.

Suspicious Activity

89. 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

90. (1) A Registrant is required to pay special attention to the above transactions by having policies, procedures and systems in place for transaction monitoring.

    (2) 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.

    (3) Registrants should note that it is insufficient to monitor only large transactions given that this would not adequately mitigate risks posed by unusual patterns of transactions and insignificant but periodic transactions 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 accounts such as accounts that have the same beneficial owner or accounts in the name of clients who are related or close associates.

(4) 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; and
(b) Known ML/TF typologies in the securities industry.

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

(6) 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.

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

Training to identify Suspicious Activity

91. Staff at all levels must be trained 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 at Appendix 3 of these AML/CFT Guidelines.

Suspicious Activity Reporting

92. A Registrant's staff must report all unusual activities or transactions to the CO immediately upon detection.
93. Due to the serious and rapid nature of ML/TF activity, it is important for the Registrant to initiate, conduct and finalise its examination required for the Registrant to establish a suspicion or reasonable grounds to suspect as quickly as possible.

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

    (a) a client'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 and no later than fourteen (14) days from the date the transaction was found to be suspicious to the FIU in the form of a SAR/STR in accordance with the FIU Regulations.

95. Registrants should implement a process for recording 'not filed' (closed, not suspicious) internal suspicious transactions/activity reports. Such records should be maintained and recorded by the CO.

96. In cases where a SAR/STR has been filed with the FIU, Registrants should continue to monitor and report any further suspicious or unusual activity in relation to that client's accounts.

97. A Registrant and/or its employees must not disclose the existence, submission or content of a SAR/STR to any person, either directly or indirectly. To do so 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.

98. 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 a group wide level. Such instances must immediately be brought to the attention of the Group CO.

99. (1) 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.

(2) On receipt of such a report the CO must consider submitting a SAR/STR to the FIU.

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

101. Copies of all documents released to the FIU pursuant to a court order being served upon a Registrant must be kept for a minimum of six (6) years from the date of release or until the original documents are returned, whichever is the later date.

Register of Enquires

102. (1) A Registrant should maintain a register of all enquiries made to them by the FIU, any law enforcement authority or other local or foreign authorities acting under powers provided by the relevant laws or their foreign equivalent, and all disclosures made pursuant to such enquiries.

(2) The register in Guideline 102 (1) above should be maintained for a minimum of six (6) years and should be kept separate from other suspicious activity/transaction records.

(3) The register in Guideline 102 (1) above should contain as a minimum requirement the following information:

(a) The date and nature of the enquiry;
(b) The details of the account(s) involved;
(c) The name and agency of the enquiring authority; and
(d) The power(s) under which the request was being made.

Tipping-off

103. Where a Registrant suspects that ML or TF 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 a SAR/STR with the FIU and should abort or abandon the CDD or EDD process.

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

105. 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.

106. A Registrant must not disclose to its client that it has reported, or intends to report, any transactions, or activity to the FIU.

PART 7: TERRORIST FINANCING

107. Registrants shall be responsible for checking the UNSCR 1267 and UNSCR 1373 lists of designated persons and entities and list of person 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 FIU in accordance with Section 22AA(2) of the ATA.

108. A Registrant must comply with Section 22AB of the ATA by following the procedures listed below upon checking the lists as stated in Guideline 107 above:

(a) Registrants must immediately inform the FIU, by using the required form which can be found on the FIU website[3]. If any person or entity named on the lists has any 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 FIU using the required form which can be found on the FIU website[4];

(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 FIU and:

[3] http://www.fiu.gov.tt/resources.php?mid=45
[4] Ibid

(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 or entity's account.

109. Staff at all levels must be trained to identify terrorist financing and must be aware of the proper procedure to be followed when terrorist financing is detected. A non-exhaustive list of indicators of Terrorist Financing can be found at Appendix 4 of these AML/CFT Guidelines.

PART 8: PROLIFERATION FINANCING

110. 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."

111. 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).

112. 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 organizations or acting as representatives or middlemen.

113. The 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 proliferation of weapons of mass destruction.

114. The role of Registrant is to implement controls to prevent access to financing by individuals and entities who may be involved in or supporting such proliferation. Even though Trinidad and Tobago does not yet have a regulatory framework for proliferation financing, it is recommended that Registrants' AML/CFT compliance programmes include PF controls, such as screening against the applicable UN lists of designated persons and countries.

APPENDIX 1

Key characteristics of the securities sector which makes it more vulnerable to ML/TF abuse:

(a) The varying roles that securities providers and other intermediaries may play in different transactions; for example, a securities provider may be both an investment fund manager and a depository bank;

(b) Differences among jurisdictions in terms of defining securities, securities products and services and their providers and the AML/CFT regulated status of these providers;

(c) ML/TF 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;

(d) Global reach of the securities sector and speed of transactions across a multitude of onshore/offshore jurisdictions and financial markets;

(e) Ability to transact in securities products via an intermediary which may provide a relative degree of anonymity;

(f) High liquidity of some securities products, which often enables their easy conversion to cash;

(g) Complex products that may be offered before they are regulated (or not regulated at all), before they are rated for ML/TF risks (e.g. the crypto-assets mentioned above), or both;

(h) Common involvement of a multitude of securities providers and intermediaries on behalf of both buying and selling principals or agents;

(i) 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;

(j) Pricing volatility of some products, particularly low priced securities;

(k) 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;

(l) Opportunity to use transactions in securities for generating illicit income within the sector, for example, market abuse or fraud; and

(m) Challenges in pricing some securities products due to their bespoke nature or complexity.

APPENDIX 2

Oversight of the AML/CFT framework

The Board of Directors of a Registrant is expected to ensure and demonstrate that there is adequate oversight of the registrant's AML/CFT framework. 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.

In order to fulfil its oversight role effectively, the Board should ensure that the reports and information that it receives adequately allows for the assessment of whether the AML/CFT 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 framework.

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

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

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

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

This additional guidance is relevant to the boards of Registrants given that Regulation 43 of the FOR creates an offence for a director of a Registrant – who directed, authorized, assented to, or acquiesced in the commission of an offence, or to whom any omission is attributable - is a party to an offence committed by the Registrant under the FOR and is liable on summary conviction or on conviction on indictment to the penalty described in section 57 of the Act.

APPENDIX 3

INDICATORS OF SUSPICIOUS ACTIVITY

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 to 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. 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 client's business or history.

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

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

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

vii. 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).

viii. 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.

ix. Quick withdrawal of funds after a very short period in the account.

x. Transfer of funds to financial or banking institutions other than those from where the funds were initially directed, specifically when different countries are involved.

xi. Transfers/journals between different accounts owned by the client with no apparent business purpose.

xii. Client requests that certain payments be routed through correspondent accounts held by the financial intermediary or sundry accounts instead of its own account.

Bearer Securities

i. The client requests cashing bearer securities without first depositing them into an account or frequently deposits bearer securities into an account.

ii. The client's explanation regarding the method of acquiring the bearer securities does not make sense or changes.

iii. The client deposits bearer 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.

Unusual Securities Transactions and Account Activity

i. Transaction where 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 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 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 organization.
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 allow 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. A 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 where 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 4

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 provide 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 organizations.

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 organizations.

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 organizations.

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 organizations.

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. 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.