GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT

MINISTRY OF FINANCE

FIU REFERENCE: GN/003/2019

GUIDANCE TO NON-REGULATED FINANCIAL INSTITUTIONS AND LISTED BUSINESS ON HOW TO STRUCTURE AN AML/CFT/PF COMPLIANCE PROGRAMME

PURPOSE

The purpose of this guidance is to assist Non-Regulated Financial Institutions (NRFIs) and Listed Businesses (LBs), collectively hereafter known as "Supervised Entities", in developing a written Compliance Programme. This Compliance Programme developed in accordance with **Section 55C of the Proceeds of Crime Act, Chap. 11:27** (as amended) ("the POCA") which contains anti-money laundering/counter financing of terrorism/proliferation financing (AML/CFT/PF/PF) measures must be approved by the Supervised Entity's senior management (directors/partners/owner of the business).

This guidance strives to explain the content of the written AML/CFT/PF Compliance Programme which should be designed as outlined in **Regulation 7 of the Financial Obligations Regulations, 2010** as amended ('the FORs"). However, a Supervised Entity is not limited from expanding their Compliance Programme to include AML/CFT/PF/PF policies that can protect the business, based on the nature of business operations.

While approval of the Compliance Programme by the FIU is no longer a requirement, the Compliance Programme will be reviewed during the conduct of a compliance examination to test the effectiveness of AML/CFT/PF measures implemented by Supervised Entities.

Table of Contents

1) INTRODUCTION 3

2) THE WRITTEN COMPLIANCE PROGRAMME 3

A. TABLE OF CONTENTS (APPENDIX I) 3

B. A POLICY STATEMENT 4

D. INTERNAL POLICIES, PROCEDURES AND CONTROLS WHICH DESCRIBES THE WHO, WHAT, WHY, WHEN AND HOW OF THE PROGRAMME 4

E. DESIGNATION OF A COMPLIANCE OFFICER (CO) AND ALTERNATE COMPLIANCE OFFICER (ACO) 7

F. ONGOING EMPLOYEE TRAINING 7

G. REVIEW OF PROGRAMME 8

1) INTRODUCTION

Legislation require that Supervised Entities register with the FIU and adopt a written AML/CFT/PF Compliance Programme which is reasonably designed to ensure proper recordkeeping and reporting of certain transactions to prevent the Supervised Entity from being used to launder money or to finance terrorism.

An AML/CFT/PF Compliance Programme should be designed to suit its individual business to address money laundering/financing of terrorism/proliferation financing (ML/FT/PF) risks identified. In developing its programme, risk factors including the size, location, complexity of business activities, cash intensity, type of products offered, and the types of transactions in which its customers engage should be considered and weighted. Once these risks are assessed the Compliance Programme should reflect the higher risk areas and the policies and procedures to mitigate the identified risks.

As evidence of approval, the written AML/CFT/PF Compliance Programme must bear the signature/stamp/seal of approval of senior management officials (directors/partners/owner of the business) and the date of approval. The policies contained in the approved Compliance Programme must be effectively communicated to all staff for immediate implementation thereafter.

This AML/CFT/PF Compliance Programme must be reviewed annually to ensure it is complies with the legal requirements and is in line with the business risk profile, incorporating benchmarking and best practice. Once gaps are identified, amendments must be made to strengthen the Compliance Programme and resubmitted to senior management for approval.

2) THE WRITTEN COMPLIANCE PROGRAMME

The written well-structured AML/CFT/PF Compliance Programme should have these five (5) key components for compliance with the national AML/CFT/PF obligations and easy to apply in practice:

a) Risk assessment

b) A system of internal compliance controls

c) Designated AML/CFT/PF compliance officer

d) Training of employees and senior management

e) Independent audit to test the system.

Any well-structured AML/CFT/PF Compliance Programme should include:

A. TABLE OF CONTENTS (APPENDIX I)

B. A POLICY STATEMENT is designed to give an outline of the purpose of the AML/CFT/PF Compliance Programme. This can include:

i. The Supervised Entity's commitment to fulfilling its AML/CFT/PF obligations and initiatives of the Government of Trinidad and Tobago in combating Money Laundering, Financing of Terrorism, proliferation financing and other related crimes.

ii. The regulatory requirements the policies and procedures developed are designed to meet e.g. FORs, Financial obligations (Financing of Terrorism) Regulations and the FIU Regulations.

iii. A statement that the Compliance Programme is designed to help employees at all levels detect and prevent money laundering, terrorist financing and proliferation financing and report same accordingly.

iv. The obligation that all employees are required to abide by the AML/CFT/PF policies and procedures **must** be made explicit.

C. OVERVIEW OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING CRIMES

i. Explain the crimes of money laundering, terrorist financing and proliferation financing. Reference can be made to the definitions stated in guidelines published by the Financial Action Task Force or other international agencies and the AML/CFT/PF legislation of Trinidad and Tobago.

ii. Explain that the laws *(The POCA, the Anti-Terrorism Act [the "ATA"] , the FORs, the FIU Act, the FIU Regulations, 2011 and the Economic Sanctions Orders),* require certain businesses to file specific reports, maintain records on certain transactions and to obtain documentation that may be used to detect, investigate and prosecute money laundering, financing of terrorism and proliferation financing crimes/offences.

D. INTERNAL POLICIES, PROCEDURES AND CONTROLS WHICH DESCRIBES THE WHO, WHAT, WHY, WHEN AND HOW OF THE PROGRAMME.

This section communicates the policies, procedures and controls that Officers and employees are expected to follow to ensure that the Supervised Entity complies with its AML/CFT legal obligations.

These Internal Policies and Controls should include:

i. A clear statement of the persons to whom the manual applies – i.e. all staff (including senior management) and all directors. Additionally, some businesses have included a declaration for staff to attest as having seen and read the Compliance Programme.

ii. Identify the Supervised Entity's responsibilities under the law including the Economic Sanctions Orders, the POCA, FIU Act and ATA and the respective Regulations**.**

iii. Identify and assess the types of ML/FT/PF risk and where the high risk activities in the organisation.

iv. Detail the Customer Due Diligence ("CDD") measures for individuals and companies. Include when these measures must be applied and the customer identification documentation required for customers (this should be based on risk. For example, valid form of national picture identification, current utility bill as proof of address, job letter or payslip as proof of employment, etc.

v. Detail measures for confirm and verify customer identification information to be carried out. This includes consulting the United Nations Sanctions List to determine whether a new or existing customer may be a designated individual or entity. Some of the United National Sanctions Lists includes:

   a. ISIL (Da'esh) Al-Qaida List (https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list);

   b. 1988 Sanctions List (https://www.un.org/securitycouncil/sanctions/1988/materials);

   c. 1518 Sanctions List (https://www.un.org/securitycouncil/sanctions/1518/materials); and

   d. 1718 Sanctions List (https://www.un.org/securitycouncil/sanctions/1718/materials).

vi. Details Enhanced Due Diligence ("EDD)" measures for high risk customers such as non-face to face customers, Politically Exposed Persons ("PEPs") persons (local or foreign), for non- residents and when business is obtained through introducers. Indicate whether copies of documentation are acceptable and whether they need to be certified and by whom. Include CDD details in accordance with Regulations 11, 12, 13, 15 and 16 of the FORs. **Sample Identification forms listing the Identification data to be collected could be attached as an Appendix.**

vii. Include the measures for monitoring of the business relationship which will identify unusual, large or suspicious business transactions.

viii. Include procedures to govern all payment methods. Is there a threshold for cash or other payment methods? Include the compulsory requirements of due diligence on:

- large transactions of TT$90, 000 and over;
- wire transfers of TT$6,000 and over;

- for private members' club transaction TT$18,000 and over; and
- occasional transactions (structured/linked transactions).

Is there a threshold for particular kind of payment method? State when a customer would be required to complete a Source of Funds Declaration ("SOFD"). **The SOFD form could be attached as an Appendix.**

ix. Include the measures to be adopted for Due Diligence for cross border business.

x. Include the EDD measures to be adopted in respect of business transactions with persons and FIs from other countries which do not sufficiently comply with the recommendations of the Financial Action Task Force.

xi. Clearly state the internal reporting procedures. The law requires the filing of a suspicious transaction/activity report (STR/SAR) with the FIU for any transaction or pattern of transactions that is attempted or conducted for ANY amount that you know or suspect or have reason to suspect :

a. Involves funds derived from a specified offence or is intended to hide funds derived from a specified offence ;

b. Is structured to avoid recordkeeping or reporting requirements;

c. Has no business or apparent lawful purpose; or

d. Facilitates criminal activity.

xii. Indicate *When* and *How* a suspicious transaction or activity will be reported to the Compliance Officer (the "CO"). **A sample form for Employees to make internal suspicious report to the CO may be attached as an Appendix.**

xiii. Include a notification to all employees that it is illegal to tell a customer that they are considering or filing a STR/SAR ("tipping-off "). 'Tipping-Off' should be clearly explained and behaviour that would constitute Tipping –Off should be illustrated.

xiv. Include a caution that Employees must not reveal the identity of the CO; his/her identity must be held in strict confidence.

xv. Maintain records of transactions and identification data for at least 6 years and for at least 6 years after relationship ends. State how they will be kept – electronic or written form. Depending on the size of the organisation, this may be a function of the Records Management department. In such case, the CO should have un-restricted access.

xvi. **An Appendix illustrating examples of suspicious activities or transactions that are <u>industry specific</u> may also be included.**

E. DESIGNATION OF A COMPLIANCE OFFICER (CO) AND ALTERNATE COMPLIANCE OFFICER (ACO)

i. Identify the level at which the designated CO and the ACO is in the Organization, (the CO should be at a responsible level, preferably at management level). It is not necessary to state CO and ACO's name in the written AML/CFT/PF Compliance Programme. The CO's and the ACO's identities and contact details **must** be provided to the FIU under separate cover. Click here

ii. State the responsibilities of the CO. The CO is responsible for the day-to-day compliance with the AML/CFT/PF's Laws and Regulations such as the Submission of STRs/SARs, Quarterly Terrorist Reports (QTRs), Terrorist Funds Reports (TFRs), where applicable and Economic Sanctions Reports (ESRs) to the FIU.

iii. Include the CO's functions under the entity's reporting obligations and specifically the following:

   a. that the STR/SAR should be in the form approved by the FIU **(You may include a copy of the form as an Appendix)**;

   b. the time within which the report must be sent to the FIU (s. 55A (3) of POCA);

   c. the reporting provisions of the ATA (both sections 33(1) and 22C of the ATA);

   d. the duty to cooperate with FIU;

   e. the duty to report BOTH **Complete and Incomplete or Declined Business**;

   f. the submission of Quarterly reports on Terrorist property ***(NRFIs only)***;

   g. the submission of a SAR if there is reasonable belief that that property is being used for terrorist activities; and

   h. the ESR report.

iv. Include other duties of the CO which may include:

   a. to monitor Lists published by the FIU, FATF, FATF Style Regional Bodies and other jurisdictions or agencies; and

   b. to keep a Register of enquiries of enquiries made by Law Enforcement Authorities and a register of STRs/SARs submitted to the FIU.

F. ONGOING EMPLOYEE TRAINING

Include measures to ensure all employees and directors are made aware of the relevant laws governing AML/CFT/PF. Measures should include:

- Provision of AML/CFT/PF training at least annually especially for personnel directly involved in the compliance function. The training should cover topic area relevant to the job function; and

- Measures of training of new employees.

The CO and the ACO will need more in depth training.

G. REVIEW OF PROGRAMME

i. The Supervised Entities must periodically assess the risk of criminal conduct and take appropriate steps to design, implement, or modify its compliance program to reduce the risk of criminal conduct identified through this process.

ii. How often? The CP must be reviewed annually to ensure its adequacy and the revised CP approved by the senior management.

iii. External Audit – Indicate how often and how it will be done, whether a written report will be prepared and to whom it will be sent.

iv. Independent Internal Audit – Indicate how often it will be conducted and whether a written report will be prepared and to whom it will be sent. By 'independent audit' is meant review, (by persons who are not part of the AML/CFT/PF compliance team of the FI's or LB's AML/CFT/PF policies and procedures), for their appropriateness, compliance and effectiveness.

Caution: Supervised Entities are required to follow all of the requirements of AML/CFT/PF laws and regulations. This guide may NOT contain all those requirements and does not create a safe harbour from regulatory responsibility. Further, an AML/CFT/PF Compliance Programme is not a **"one-size-fits-all"**, and **you must tailor your plan to fit your particular financial institutions' or listed business operations and strategic objectives.**

Dated May 28, 2019

Nigel Stoddard
Director (Ag.)
Financial Intelligence Unit

****

End of document

Appendix I

COMPLIANCE PROGRAMME

TABLE OF CONTENTS

1. INTRODUCTION
   - 1.2 Policy Statement *(Purpose of the Compliance Programme)*
   - 1.3 Nature of Business *(What are the core and related business activities)*
   - 1.4 Overview of Money Laundering/Terrorist Financing/Proliferation Financing
   - 1.5 Legislative Framework *(Brief summary of AML/CFT legislative regime of Trinidad and Tobago)*

2. RISK BASED APPROACH *(Regulation 14 of the FORs)*
   - 2.2 Categories of Risk *(Based on Product, Payment Methods, Customers, Jurisdictions, etc)*
   - 2.3 High Risk Customers, Transactions and Activities

3. INTERNAL CONTROLS
   - 3.2 Customer Due Diligence Measures
     - 3.2.1 Individual customer identification *(Regulations 11 and 15 of the FORs)*
     - 3.2.2 Business Customers *(Regulations 11, 12 and 16 of the FORs)*
   - 3.3 Enhanced Due Diligence
     - 3.3.1 Third Party Transactions
     - 3.3.2 Politically Exposed Persons
     - 3.3.3 Non Face-to-Face Transactions/Relationships
   - 3.4 Compliance and alternate Compliance Officer
     - 3.4.1 Appointment and Approval *(Regulation 3 and 4 of the FORs)*
     - 3.4.2 Duties and Responsibilities *(Regulation 4 of the FORs)*
   - 3.5 Payment Policy
     - 3.5.1 Transaction Threshold (Cash, Wire Transfers, etc)
     - *3.5.2* Source of Funds Declarations *(Regulation 15 (h) of the FORs)*
   - 3.6 Record Keeping Obligations

4. REPORTING OBLIGATIONS
   - 4.2 Internal Reporting Measures *(Procedures for identification and reporting to the Compliance Officer)*
   - 4.3 Decision Making Process
   - 4.4 Indicators *(What are the red flags for your business)*
   - 4.5 Transaction Monitoring
   - 4.6 Reporting to the FIU

5. TRAINING AND RECRUITMENT
   - 5.2 Training of Staff *(Regulation 6 of the FORs)*
   - 5.3 Ongoing Training (Frequency and type of training)

6. INDEPENDENT TESTING
   - 6.2 Period of Review
   - 6.3 Selection of an auditor
   - 6.4 Timeline for reporting

7. Appendices

SAMPLE