GUYANA SECURITIES COUNCIL

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM FOR REPORTING ENTITIES WITHIN THE SECURITIES SECTOR

GUIDELINE NO. 1 OF 2023

30/01/2023 This document is applicable to reporting entities who are supervised under the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 as amended (AMLCFT Act), by the Guyana Securities Council, a supervisory authority pursuant to Section 22(1)(c) of the AML/CFT Act and is issued pursuant to Section 22(2)(b) of the AML/CFT Act and Regulation 19(1) of the AML/CFT Regulation No. 4 of 2010.

CONTENTS

CHAPTER 3-REQUIREMENTS AND OBLIGATIONS OF REPORTING ENTITIES

CHAPTER 4 - LIABILITY, SANCTIONS & INFORMATION SHARING

CHAPTER 5 - EMERGING ML/TF/PF CHALLENGES & THREATS

Foreword

This Anti-Money Laundering and Countering the Financing of Terrorism (AMLCFT) Guideline is issued by the Guyana Securities Council (GSC). It aims to ensure that reporting entities falling under the supervision of the Guyana Securities Council (GSC) effectively comply with their obligations under the AML/CFT legislation and meet international best practices within the securities sector.

This Guideline is designed to assist reporting entities within the securities sector to promote a better understanding of their AMLCFT obligations and requirements.

This Guideline must be used in conjunction with any other relevant Guideline issued by the Financial Intelligence Unit (FIU) and the AMLCFT laws, and if found to be inconsistent with any written law or regulation, that law or regulation shall take precedent.

INTRODUCTION

The Guyana Securities Council (GSC) holds a primary mandate as the regulatory body for the securities sector in Guyana pursuant to **Section 4 of the Securities Industry Act, 1998 and Regulations** thereunder. The Guyana Securities Council (GSC) pursuant to **Section 22(1)(c) of the AMLCFT Act**, as amended, holds a secondary mandate as the designated supervisory authority for securities related activity as set out in the **Fourth Schedule of the AMLCFT Act**.

The GSC plays an integral role within the financial sector in combatting money laundering, terrorist financing and proliferation financing through its regulatory and supervisory roles in Guyana's comprehensive AML/CFT/PF framework.

This Guideline is specifically targeted to reporting entities falling under the supervision of the GSC as set out and contemplated under the **AMLCFT Act, as amended**, in conjunction with the **Securities Industry Act, 1998 and Regulations** thereunder.

LEGISLATIVE FRAMEWORK

There are several relevant and pertinent pieces of legislation referenced in this Guideline. The principal Acts being the **Anti-Money Laundering and Countering the Financing of Terrorism Act, 2009 (as amended) (AMLCFT Act) and the Securities Industry Act, 1988 (SIA).**

There have been several legislative amendments to the **AMLCFT Act, 2009**. As such these legislative improvements include the following enactments:

- **AMLCFT Amendment Act No. 15 of 2010**
- **AMLCFT Amendment Act No. 1 of 2015**
- **AMLCFT Amendment Act No. 10 of 2015**
- **AMLCFT Amendment Act No. 15 of 2016**
- **AMLCFT Amendment Act No. 21 of 2017**
- **AMLCFT Amendment Act No. 17 of 2018**
- **AMLCFT Amendment Act No. 12 of 2022**
- **AMLCFT Regulation No. 4 of 2010**
- **AMLCFT Regulation No. 4 of 2015**
- **AMLCFT Regulation No. 7 of 2015**
- **Guidance Note on Securities Companies Guideline No. 4 of 2016** issued by the FIU
- **FIU AMLCFT Handbook for Reporting Entities** published 18th February, 2021

This Guideline seeks to incorporate these amendments in a comprehensive manner to assist reporting entities within the securities sector.

CHAPTER 1- RELEVANT ENTITIES & COMPETENT AUTHORITIES

SUPERVISORY AUTHORITY

Who is a supervisory authority?
A supervisory authority means the authority set out in **Column 2 of the Fourth Schedule** who has compliance oversight over a reporting entity set out in **Column 1 of the Fourth Schedule**.

The Guyana Securities Council (GSC) is a supervisory authority pursuant to **Section 22(1)(c) of the AMLCFT Act, as amended**, and **Section 6(bA) of the Securities Industry Act**, amended by **Section 25 of the AMLCFT Amendment Act No. 1 of 2015.**

Supervisory authorities are responsible for supervising compliance by their respective Reporting Entities with the requirements of the AMLCFT legislation.

The GSC is the supervisory authority for reporting entities who carry on the following activity or business:

- **Trading for own account or for account of customers in money market instruments (such as cheques, bills, certificates of deposit), foreign exchange, financial futures and options, exchange and interest rate instruments, and transferrable securities,**
- **Underwriting share issues and participation in such issue,**
- **Advice to undertakings on capital structure, industrial strategy and related questions, and advice and services relating to mergers and the purchase of undertakings,**
- **Money broking,**
- **Portfolio management and advice,**
- **Safekeeping and administration of securities,**
- **Venture risk capital,**
- **Unit trusts.**

What are the responsibilities of the GSC as a supervisory authority?

The responsibility of the GSC is outlined in **Section 22(2) of the AMLCFT Act**, as amended and is the same as applicable to all supervisory authorities, and includes but is not limited to:

(a) Examining and supervising the reporting entity, and regulating and overseeing effective compliance with the obligations set out in **Sections 15, 16, 18, 19 and 20** and any other preventive measures in relation to combating money laundering and terrorist financing;

(b) Issuing instructions, guidelines or recommendations and provide training to reporting entities on their obligations and requirements under the AMLCFT Act and to make the reporting entities aware of any amendments to the laws relating to money laundering, terrorist financing or proceeds or crime;

(c) Ensuring that their respective Reporting Entities update their AML/CFT policies in accordance with AML/CFT legislative amendments;

(d) Developing standards and criteria applicable to the communication of suspicious activities that reflect other existing and future pertinent national and internationally accepted standards; and

(e) Imposing requirements that the Reporting Entity shall ensure that their foreign branches and subsidiaries adopt and enforce measures consistent with this Act to the extent that local laws and regulations so permit, and where the foreign branch or subsidiary is unable to adopt and observe these measures, to report the matter to the designated supervisory or regulatory authority or the competent disciplinary authority.

In order to secure compliance by their respective Reporting Entities with the requirements of the AMLCFT legislation, supervisory authorities have the authority to –

(a) **Enter** in the business premises of their respective Reporting Entity during ordinary working hours in order to inspect or take documents or make copies or extracts of information from such documents, inspect premises, and observe the manner in which certain functions are undertaken[1];

(b) **Require** any person on the premises to provide an explanation on any such information[2]; and

(c) **Request** and be given information relevant to money laundering and terrorist financing matters from their respective Reporting Entities.[3]

REPORTING ENTITIES

Who is a reporting entity?

Section 2 of the AMLCFT Act 2009, as amended, defines a reporting entity to mean 'any person (legal or natural person) whose regular occupation or business is the carrying on of –

(a) Any activity listed in the First Schedule; or

[1] Section 22(2)(bA)(a) of the AMLCFT Act as amended.
[2] Section 22(2)(bA)(b) of the AMLCFT Act as amended.
[3] Section 22(2)(bB) of the AMLCFT Act as amended.

(b) Any other activity defined by the Minster responsible for Finance as such by an order published in the Gazette amending the First Schedule.'

The term **'financial institution'** is given a wide meaning under the **AMLCFT Act, as amended**, and it is different from the meaning under the **Financial Institutions Act**. For the purpose of this Guideline, the definition used and adopted is the definition as set out in the **AMLCFT Act, as amended**.

The **First Schedule** of the **AMLCFT Act** sets out the scope of **'financial institutions'** who are deemed **'reporting entities'** pursuant to **Section 2 of the AMLCFT Act**, as amended. This includes the following types of persons, companies or businesses that engage in any of the following activities: -

(a) Acceptance of deposits and other repayable funds from the public, including but not limited to private banking,
(b) Lending, including but not limited to customer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions including forfaiting,
(c) Financial leasing other than with respect to arrangements relating to consumer products,
(d) The transfer of money or value,
(e) Issuing and managing means of payment, including, but not limited, to credit cards, travelers' cheques, money orders and bankers' drafts, and electronic money,
(f) Issuing financial guarantees and commitments
(g) Trading in-
    a. Money market instruments, including but not limited to-cheques, bills, certificates of deposit and derivatives,
    b. Foreign exchange,
    c. Exchange, interest rate and index instruments,
    d. Transferrable securities, and
    e. Commodity futures trading,
(h) Participating in and underwriting securities issues and the provision of financial services to such issue,
(i) Individual and collective portfolio management,
(j) Safekeeping and administration of cash or liquid securities on behalf of other persons,
(k) Investing, administering or managing funds or money on behalf of other persons,
(l) Underwriting and placement of life insurance and other investment-related insurance, as well as insurance intermediation by agents and brokers,
(m) Money and currency changing, and
(n) Such other activity, business or operation as may be prescribed by the Minister responsible for Finance.

For the purposes of this Guideline, Designated Non-Financial Businesses and Professions (DNFBPs) will not be addressed as they are not supervised by the GSC under **Section 22(1)(c) of the AMLCFT Act, as amended**.[4]

[4] For further details on DNFBPs see First Schedule of the AMLCFT Act, as amended.

Further, the **First Schedule** prescribes the type of activities and businesses that are subject to supervisory oversight under the AMLCFT framework. For the application and purpose of this Guideline, **only financial activities** are specified below are supervised by the GSC and includes the following: -

- Acceptance of deposits and other repayable funds from the public,
- Lending, including consumer credit, mortgage credit, factoring (with or without recourse) and financing of commercial transactions,
- Financial leasing,
- Money transfer agencies or services, including money exchanges,
- Issuing and administering means of payment (such as credit cards, travelers' cheques, and bankers' drafts,
- Guarantee and commitments
- Trading for own account or for account of customers in money market instruments (such as cheques, bills, certificates of deposit), foreign exchange, financial futures and options, exchange and interest rate instruments, and transferrable securities,
- Credit unions,
- Underwriting share issues and participation in such issues,
- Advice to undertakings on capital structure, industrial strategy and related questions, and advice and services relating to mergers and the purchase of undertakings,
- Money broking
- Portfolio management and advice (investment advisory)*
- Safekeeping and administration of securities and safe custody services
- Insurance business
- Venture risk capital
- Unit trusts.

ROLE OF THE FINANCIAL INTELLIGENCE UNIT (FIU)

The Financial Intelligence Unit (FIU) of Guyana plays a central role in Guyana's AML/CFT operational network and provides support to the work of other competent authorities. The FIU is established and operates under **Section 9 (1) of the AML/CFT Act 2009, as amended**.

Core functions

The core functions of the FIU are outlined under **Section 9(4) of the AMLCFT Act**. Central to these functions, is the FIU's primary responsibility to request, receive, analyze and disseminate information in the form of intelligence reports based on suspicious transactions and other information submitted by reporting entities and other competent authorities.

The FIU's core function is supported by the cooperation and collaboration with reporting entities, supervisory authorities, and other competent authorities such as the Special Organised Crime Unit (SOCU), Guyana Revenue Authority (GRA), the Land, Deeds and Commercial Registries, to gather intelligence

within the AML/CFT framework and analyze and disseminate information as may be necessary to fulfill its overall mandate under the AMLCFT Act.

Other functions

Some other functions of the FIU include:

- Maintaining statistics and records;
- Issuing guidelines to reporting entities;
- Providing advice to the Minister of Finance on matters relating to ML or TF that affect public policy or national security;
- Conducting of research into trends and developments to improve ways of detecting, preventing and deterring money laundering and terrorist financing;
- Creating training requirements and providing training for reporting entities on identification, record keeping and reporting obligations under AMLCFT Act;
- Conducting investigations into money laundering, proceeds of crime and terrorist financing (for official purposes only); and
- Extending legal assistance to foreign jurisdiction with respect to production orders, property tracking, monitoring, forfeiture or confiscation orders.

CHAPTER 2 - MONEY LAUNDERING, TERRORISM FINANCING, PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS

MONEY LAUNDERING

What is money laundering?

Money laundering is defined in **Section 2 of the AMLCFT Act, as amended**, to mean conduct which constitutes an offence as described in **Section 3 of the AMLCFT Act**.

The money laundering process is often described as taking place in three stages: Placement, Layering and Integration.

Placement

During this stage, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international.

Examples of placement transactions include:

- Blending of funds: Commingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned businesses.
- Foreign exchange: Purchasing of foreign exchange with illegal funds.
- Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements.
- Currency smuggling: Cross-border physical movement of cash or monetary instruments.
- Loans: Repayment of legitimate loans using laundered cash.

Layering

This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to conceal or obscure the true source and/ or ownership of funds.

Examples of layering transactions include:

- Electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
- moving funds from one financial institution to another or within accounts at the same institution; converting the cash placed into monetary instruments;
- reselling high-value goods and prepaid access/stored value products;
- investing in real estate and other legitimate businesses
- placing money in stocks, bonds or life insurance products; and
- using shell companies to obscure the ultimate beneficial owner and assets.

Integration

This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets.

Example of integration transactions include:

- Getting into financial arrangements or other ventures where investments can be made in business enterprises, venture risk and start up ventures where a large capital investment is required.

MONEY LAUNDERING IS AN OFFENCE

Pursuant to the **AMLCFT Act**, money laundering means conduct which constitutes an offence as described under **Section 3 of the Act**.

Section 3(1) provides "A person commits the offence of money laundering if he knowingly or having reasonable grounds to believe that any property in whole or in part directly or indirectly represents any person's proceeds of crime –

(a) converts or transfers property knowing or having reason to believe that property is the proceeds of crime, with the aim of concealing or disguising the illicit origin of that property;

(b) conceals or disguises the true nature, origin, location, disposition, movement or ownership of that property knowing or having reason to believe that the property is the proceeds of crime;

(c) acquires, possesses or uses that property, knowing or having reasonable grounds to believe that it is derived directly or indirectly from proceeds of crime;

(cA) assists any person who is involved in the commission of an offence in paragraphs (a), (b), or (c) to evade the legal consequences of his actions; or

(d) participates in, associates with or conspires to commit, attempts to commit or aids and abets, counsels or procures or facilitates the commission of any of the above acts."

Sections 3(6) and (7) of the AML/CFT Act provides:

(a) A natural person who contravenes this section commits an offence and shall be liable:

(i) on summary conviction, to a fine of not less than **five million dollars (GY$5,000,000)** nor more than **one hundred million dollars (GY$100,000,000)** and to imprisonment for **seven (7) years**, or

(ii) on conviction on indictment, to a fine of not less than **ten million dollars (GY$10,000,000)** nor more than **one hundred and twenty million dollars (GY$120,000,000)** and to imprisonment for **ten (10) years**.

(b) A body corporate which contravenes this section commits an offence and shall be liable:

(i) on summary conviction, to a fine of not less than **two hundred million dollars (GY$200,000,000)** nor more than **five hundred million dollars (GY$500,000,000)**; or

(ii) on conviction on indictment to a fine of not less than **two hundred and twenty million dollars (GY$220,000,000)** nor more than **five hundred and twenty million dollars (GY$520,000,000)**.

See the FIU website for further details: **https://fiu.gov.gy/cfatf-publications/**

TERRORISM FINANCING

What is terrorism financing?

Sections 67-75 of the AMLCFT Act, as amended, set out the law in relation to terrorism financing (inclusive) and means willfully providing or collecting funds, whether from a legitimate or an illegitimate source, by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be use in full or in part:

a) To carry out, terrorist acts[5]
b) By a terrorist organization[6], or
c) By an individual terrorist

What is a terrorist act?

A terrorist act is any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or international organization to do or to abstain from doing any act[7].

Further, **Section 2 of the AMLCFT Act, as amended** defines **'terrorist act'** – having the same meaning assigned to it as in the **Criminal Law (Offences) Act**, of the laws of Guyana, **and** includes-

(a) Any act which constitutes an offence within the scope of, and as defined in any of the following treaties-

i. **The Convention for Suppression of Unlawful Seizure of Aircraft (1970)**

ii. **The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)**

iii. **The Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973)**

iv. **The International Convention against Taking of Hostages (1979)**

v. **The Convention on the Physical Protection of Nuclear Material (1980)**

vi. **The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Act Against the Safety of Civil Aviation (1988)**

[5] Terrorist act is defined in Section 2 of the AMLCFT Act

[6] Terrorist organization defined in Section 2 of the AMLCFT Act – means any group of terrorists that- (a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully, (b) participates as an accomplice in terrorist acts, (c) organizes or directs others to commit terrorist acts, or (d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

[7] Section 2 of AMLCFT Act, as amended.

vii. **The Convention for the Suppression of Unlawful Act against the Safety of Maritime Navigation (1988)**

viii. **The Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and**

ix. **The International Convention for the Suppression of Terrorist Bombings (1997).**

Who is a terrorist?[8]

The term terrorist refers to any natural person who:

a) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;
b) participates as an accomplice in terrorist acts;
c) organizes or directs others to commit terrorist acts; or
d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

What is a terrorist organization[9]**?**

The term terrorist organization refers to any group of terrorists that

(i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;
(ii) participates as an accomplice in terrorist acts;
(iii) organizes or directs others to commit terrorist acts; or
(iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

What is considered terrorist property?

Section 2 of the AMLCFT Act, as amended defines '**terrorist property'** to mean –

a) Proceeds from the commission of terrorism,
b) Money or other property which has been, or is likely to be used to commit terrorism, or
c) Money or other property which has been, is being or is likely to be used by a terrorist group.

TERRORIST FINANCING: A CRIMINAL OFFENCE

Section 68(1) of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act 2009 as amended provides:

[8] Section 2 of AMLCFT Act, as amended
[9] ibid

A person who by any means directly or indirectly, willfully provides or collects funds or other property, with the intention that they should be used or in the knowledge that they are to be used in whole or in part –

(a) to commit an act constituting an offence in regard to and in accordance with the definition of one of the treaties listed in the appendix to the International Convention for the Suppression of the Financing of Terrorism to which Guyana is a party;
(b) to commit any act intended to cause the death of or serious bodily injury to any civilian or any other person not directly involved in a situation of armed conflict if, by virtue of its nature or context, such act is intended to intimidate a population or compel a government or international organization to perform or refrain from performing an act of any kind;
(c) by a terrorist;
(d) by a terrorist organization; or
(e) to finance the travel of any person who travels to a country other than their country of residence or nationality for the purpose of perpetrating, planning, preparing or participating in terrorist act, or providing or receiving terrorist training, commits an indictable offence and shall –
    (i) if such act resulted in the death of any person, be punishable with a fine of not less than **one million five hundred thousand dollars (GY$1,500,000) together with death**;
    (ii) in any other case, the punishment is a fine of not less than **five hundred thousand dollars (GY$500,000)** together with imprisonment for not less than **ten (10) years** nor more than **fifteen (15) years**.

For further information see:

1) Detecting or Preventing Terrorist Financing Guideline No. 1 of 2018 issued by the FIU
2) **FIU website for further details:** **https://fiu.gov.gy/cfatf-publications/**
3) **See Annex B attached.**

PROLIFERATION FINANCING

What is proliferation financing?

According to **Section 2(1) of the AML/CFT Act 2009 as amended 'proliferation financing'** includes 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 nonlegitimate purposes), in contravention of national laws or, where applicable, international obligations.

PROLIFERATION FINANCING: A CRIMINAL OFFENCE

According to **Section 68E(12) of the AML/CFT Act 2009 as amended**, a natural person who commits this offence shall be liable on summary conviction to a fine of not less than **five million dollars (GY$5,000,000)** nor more than **one hundred millions dollars (GY$100,000,000)** or to imprisonment for

up to **seven (7) years** and in the case of a body corporate to a fine of not less than **ten million dollars (GY$10,000,000)** nor more than **two hundred million dollars (GY$200,000,000)**.

For further information visit the FIU's website: https://fiu.gov.gy/cfatf-publications/

TARGETED FINANCIAL SANCTIONS RELATED TO TERRORISM, TERRORISM FINANCING AND PROLIFERATION FINANCING

The AML/CFT legislation establishes a legal framework for asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of a listed person or entity.

A listed person or entity is:

(i) Any person or entity designated pursuant to **United Nations Security Council Resolution (UNSCR) 1267/1999** and its successor resolutions;
(ii) Any person or entity specified by Guyana pursuant to **UNSCR 1373(2001)** and its successor resolutions;
(iii) Any person or entity designated by the **1718 Sanctions Committee of the Security Council** in accordance with **UNSCR 1718 (2006)** and its successor resolutions; or
(iv) Any person or entity designated by the **2231 Sanctions Committee** in accordance with **UNSCR 2231(2015)** and its successor resolutions.

Prohibitions/Freezing Requirement

A person or entity including a reporting entity is prohibited from knowingly –

(a) Dealing directly or indirectly with any funds or other assets of a listed person or entity.
(b) Entering into or facilitating, directly or indirectly, any transaction related to a listed person or entity.
(c) Providing any financial or other related services in respect of funds or other assets of a listed person or entity.
(d) Making any property or any financial or other related service available, directly or indirectly, for the benefit of a listed person or entity.

Once it is established that a customer is a listed person or entity, the reporting entity must immediately inform the Director-FIU.

For further information see:

1) **Guide on Implementing Targeted Financial Sanctions Measures Guideline No. 2 of 2015** issued by the FIU

2) **Targeted Financial Sanctions related to Terrorism and Terrorism Financing Guideline No. 3 of 2015** issued by the FIU
3) **Targeted Financial Sanctions related to Terrorism, Terrorism Financing and Proliferation Financing Guideline No. 1 of 2022** issued by the FIU.

CHAPTER 3 - REQUIREMENTS AND OBLIGATIONS OF REPORTING ENTITIES

APPOINT A COMPLIANCE OFFICER

Appoint Or Designate A Compliance Officer Who Shall Be Responsible For Ensuring The Reporting Entity's Compliance With The Requirements Of The AML/CFT Legislation[10];

The appointed or designated compliance officer must have responsibility for ensuring the reporting entity's compliance with the requirements of the AML/CFT legislation.

The compliance officer must be at the management level with appropriate and adequate authority and responsibility to implement the AML/CFT legislative provisions.
The compliance officer must therefore –

(i) be a senior officer with relevant qualifications and experience to enable him/her to respond sufficiently well to enquires relating to the reporting entity and the conduct of its business;
(ii) be responsible for establishing and maintaining a manual of compliance procedures in relation to the business of the reporting entity;
(iii) be responsible for ensuring compliance by staff of the reporting entity with-
    a. the provisions of the AML/CFT legislation;
    b. the provisions of any manual of compliance procedures established by the reporting entity; and
    c. the internal reporting procedures established in accordance with the AML/CFT legislation.
(iv) act as the liaison between the reporting entity and the FIU in matters relating to compliance with the provisions of the AML/CFT legislation with respect to ML or TF;
(v) prepare and submit reports to the FIU on the reporting entity's compliance with the AML/CFT legislation; and
(vi) have the authority to act independently and to report to senior management above the compliance officer's next reporting level and the board of directors or equivalent body.

[10] Section 19(1)(a) of the AMLCFT Act as amended.

ESTABLISH AND MAINTAIN INTERNAL POLICIES, PROCEDURES, CONTROLS AND SYSTEMS[11]

The reporting entities policies, procedures, controls and systems should outline how the reporting entity will:

(a) undertake risk assessments of its business and its customers;

(b) enable all its directors or, as the case may be partners, all other persons involved in its management, and all key staff to know to whom they should report any knowledge or suspicion of money laundering, proceeds of crime or terrorist financing activity;

(c) ensure that there is a clear reporting chain under which suspicions of money laundering, proceeds or crime or terrorist financing activity will be reported to the compliance officer;

(d) identify a compliance officer to whom a report is to be made or any information or other matter which comes to the attention of the person handling that business and which in that person's opinion gives rise to knowledge or suspicion that another person is engaged in money laundering, proceeds or crime or terrorist financing;

(e) require the compliance officer to consider any report in light of all other relevant information available to that compliance officer for the purpose of determining whether or not it gives rise to knowledge or suspicion of money laundering, proceeds or crime or terrorist financing;

(f) ensure that the compliance officer has reasonable access to any other information which may be of assistance to him/her and which is available to the reporting entity;

(g) require that the information or other matter contained in a report is disclosed promptly to the FIU where there is a suspicion of money laundering, proceeds or crime or terrorist financing activity;

(h) determine the true identity of customers and any beneficial owners and controllers;

(i) determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;

(j) require identification information to be accurate and relevant;

(k) require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to all complex, unusual large business transactions, unusual patterns of transactions, whether completed or not, which have no apparent economic or lawful purpose and inconsistent with the profile of the person(s) carrying out such transactions;

(l) compare expected activity of a customer against actual activity;

(m) apply increased vigilance to transactions and relationships posing higher risks of ML/TF;

(n) ensure adequate resources are available for the entity's independent audit function to test and monitor its AML/CFT procedures and systems;

[11] Section 19(1)(b) of the AMLCFT Act as amended.

(o) ensure procedures are established and maintained which allow the compliance officer to have access to all relevant information, which may be of assistance to them in considering suspicious transaction reports ("STRs");

(p) require a disclosure to the FIU when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and/or TF, including attempted ML and/or TF;

(q) maintain records for the prescribed periods of time; and

(r) require the screening of persons before hiring them

For further details see:
Policy Manual-Guidance Notes No 1 of 2017 issued by the FIU.

IMPLEMENT AN INDEPENDENT AUDIT FUNCTION

Establish And Maintain Independent Audit Function to test its AMLCFT Procedures And Systems[12];

(a) The independent audit should at a minimum:

(b) Assess the overall integrity and effectiveness of the AML/CFT compliance program, including policies, procedures and processes.

(c) Assess the adequacy of the AML/CFT risk assessment.

(d) Examine the adequacy of CDD policies, procedures and processes, and whether they comply with regulatory requirements.

(e) Determine personnel adherence to the entity's AML/CFT policies, procedures and processes.

(f) Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations).

(g) Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.

(h) Assess compliance with the AML/CFT Act, Regulations and Guidelines.

(i) Examine the integrity and accuracy of management information systems used in the AML/CFT compliance program.

(j) Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the FIU.

(k) Assess the effectiveness of the entity's policy for reviewing accounts/transactions that generate multiple suspicious transaction report filings, including account closure processes.

(l) Assess the adequacy of record-keeping and record retention processes.

[12] Section 19(1)(c) of the AMLCFT Act as amended.

(m) Track previously identified deficiencies and ensure management corrects them promptly.

(n) Consider whether the management of the entity was responsive to earlier audit findings.

(o) Determine the adequacy of the following, as they relate to the training program and materials:

- The importance the board and senior management place on ongoing education, training and compliance.
- Employee accountability for ensuring AML/CFT compliance, including the employee performance management process.
- Comprehensiveness of training related to the risk assessment of each individual business line.
- Training of personnel from all applicable areas of the entity. • Frequency of training including the timeliness of training given to new and transferred employees
- Coverage of internal policies, procedures, processes and new rules and regulations.
- Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.
- Disciplinary actions taken for noncompliance with internal policies and regulatory requirements

CONDUCT AML/CFT TRAINING[13]

AML/CFT training should be designed to improve the knowledge, performance and skills of employees by enhancing their understanding of relevant laws, regulations, guidelines, and the reporting entity's internal policies, controls and systems.

Who should be trained?

- Directors, partners, senior management staff of the entity
- Customer facing staff
- AML/CFT Compliance staff

What to train on?

At a minimum the content of training should include:

- The AML/CFT Act, Regulations and Guidelines.
- Employees obligations under the AML/CFT legislation.

[13] Section 19(1)(d) of the AMLCFT Act as amended

- The Entities policies and procedures to prevent ML/TF.
- The Entity's customer identification, record keeping and other procedures.
- How to recognize and handle suspicious activities.
- International standards that drive domestic requirements.
- The potential ML/TF risks to the entity that have been determined from the entity's risk assessment.
- Feedback on AML/CFT issues arising from supervisory, audit or regulatory reports.

When to train?

Training should be an ongoing process that should be updated regularly **(at least once every year)** to reflect current developments and changes to laws and regulations and the reporting entities' business environment and the type of customers.

REGISTER WITH THE FIU

Register with the FIU In Such Manner And Form As Determined By The Director[14]

All reporting entities are required to register with the FIU. This is to facilitate monitoring of the reporting entity's compliance with the provisions of the AML/CFT legislation.

Requirement:

1. Completed Registration Form (Form must be signed and dated)
2. Copy of Identification for owners/directors/senior executives/trustees (whichever is applicable)
3. Copy of entity's business registration/certificate of incorporation document/partnership agreement (including any governing documents e.g. Constitution/By-laws/Rules)
4. Copy of entity's operations registration/license
5. Copy of entity's most recent Financial Statement or Annual Returns. Cost – Registration is FREE Registration Form is available on the FIU's website – fiu.gov.gy

ASSESS RISKS AND APPLY A RISK-BASED APPROACH[15]

Risk Assessment of Reporting Entities within the Securities Sector

[14] Section 19(4) of the AMLCFT Act as amended.
[15] Section 19(1)(e) of the AMLCFT Act as amended.

Reporting entities are required to take appropriate steps to identify, assess and understand their money laundering and terrorist financing risks for customers, countries or geographic areas; and products, services, transactions or delivery channels. The risk assessments must be documented and kept up to date.

Combating ML/TF is a global priority. The risk assessment should enable the reporting entity to understand how, and to what extent, it is vulnerable to ML/TF. The risk assessment will also be developed because of regulatory requirements, guidance or expectations and will form the basis of a reporting entity's RBA. It will often result in the categorization of risks, including inherent and residual risks based on established controls and other mitigants, which will help reporting entities to determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk.

The risk assessment should be properly documented, regularly updated and communicated to the relevant reporting entity's senior management. In conducting their risk assessments, reporting entities should consider quantitative and qualitative information obtained from relevant internal and external sources to identify, manage and mitigate these risks. This may include consideration of the risk and threat assessments, crime statistics, typologies, risk indicators, red flags, guidance and advisories issued by inter-governmental organisations, national competent authorities and the FATF, and AML/CFT mutual evaluation and follow-up reports by the FATF or associated assessment bodies. This may be accessed on the Financial Intelligence Unit's website under publications.

Furthermore, in identifying and assessing indicators of ML/TF risk to which it is exposed, a reporting entity should consider a range of factors including:

a) The nature, diversity and complexity of its business, products and target markets;
b) The proportion of customers identified as high risk
c) The jurisdictions in which the reporting entity is operating or otherwise exposed to, either through its own activities or the activities of customers, especially jurisdictions with greater vulnerability due to contextual and other risk factors such as the prevalence of crime, corruption, or financing of terrorism, the general level and quality of the jurisdiction's prosecutorial and law enforcement efforts related to AML/CFT, the regulatory and supervisory regime and controls and transparency of beneficial ownership;
d) The distribution channels through which the securities provider distributes its products, including the extent to which the securities provider deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD or other AML/CFT obligations, the complexity of the transaction chain (e.g. layers of distribution and sub-distribution, type of distributors such as independent financial advisors, investment advisors) and the settlement systems used between operators in the payment chain, the use of technology and the extent to which intermediation networks are used;
e) The internal and external (such as audits carried out by independent third parties, where applicable) control functions and regulatory findings; and
f) The expected volume and size of its transactions, considering the usual activity of the reporting entity and the profile of its customers.

Reporting Entities should review their assessments periodically and when their circumstances change or relevant new threats emerge. Reporting Entities should consider internal feedback within their organization, including from those who interact with customers, compliance risk management, and internal audit departments (where relevant), in performing their periodic risk assessments.

ML/TF risks may be measured using various methods. The use of risk categories enables reporting entities to manage potential risks by subjecting customers to proportionate controls and oversight. The most commonly used risk criteria are: country or geographic risk; customer/investor risk; product/service risk and intermediary risk.

The extent to which these risk categories are applicable and the weight they should carry (individually or in combination) in assessing the overall risk of potential ML/TF risk may vary from one institution to another, depending on their respective circumstances and risk management framework. Reporting entities must comprehensively review all risk factors relevant to their business, including how certain factors may interplay and have an amplifying effect. For example, the risks inherent in an under-developed securities sector could be amplified by regional risks (if it is located, e.g. in an area where there is high incidence of drug trafficking). Consequently, reporting entities should determine the risk weights and at the same time, parameters set by law or regulation may limit a business's discretion.

There are no complete set of risk categories, however the most commonly identified are:

- Country/ Geographic Risk
- Customer/ Investor Risk
- Product/ Service/ Transactions Risk
- Distribution Channel Risk

See Annex B below for further details.

Having assessed ML/TF risks in their business, Reporting entities in the securities sector should then develop mitigating controls proportionate to the ML/TF risks identified and to the complexity, nature and size of the entity and activity. Consistent with the RBA, reporting entities should allocate more resources to mitigating their most significant risks.

Reporting Entities should apply appropriate Countermeasures To Higher-Risk Countries[16]

Reporting entities are required to apply enhanced due diligence measures to business relationships and transactions with customers from countries for which this is called for by the Financial Action Task Force (FATF). The type of enhanced measures should be effective and proportionate to the risks.

Note: The FIU advises reporting entities, through their respective supervisory authority, in this case the Guyana Securities Council of higher risk countries - countries with strategic AML/CFT deficiencies that FATF identifies as:

[16] Section 16(7) of the AMLCFT Act as amended by Section 10 of the AMLCFT Amendment Act No. 1 of 2015

(i) High-Risk Jurisdictions subject to a Call for Action, and
(ii) Jurisdictions under Increased Monitoring.

Reporting Entities should identify and assess ML/TF Risks related to New Technologies[17]

Reporting entities must identify and assess the money laundering or terrorist financing risks that may arise in relation to –

(a) The development of new products and new business practices, including new delivery mechanisms; and
(b) The use of new or developing technologies for both new and pre-existing products.

Further:

(a) The risk assessments must be undertaken prior to the launch or use of new or developing technologies or products, and

Appropriate measures must be in place to manage and mitigate any identified risks.[18]

CUSTOMER DUE DILIGENCE

Reporting Entities must identify and verify the identity of customers pursuant to Section 15 of the AMLCFT Act 2009 as amended.

The process of identifying and verifying the identity of a customer is commonly referred to a "customer due diligence" or "know your customer" (CDD / KYC). A reporting entity must carry out standard customer due diligence (CDD) for all its customers.

The CDD process should assist reporting entities to assess ML/TF risk associated with a business relationship. Reporting Entities should have policies, procedures, systems and controls which are up to date and effectively implemented to carry out CDD.

Standard CDD measures include:

- Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.
- Identifying the beneficial owner and taking reasonable measures on a risk-sensitive basis to verify the identity of the beneficial owner, such that the reporting entity is satisfied about the identity of beneficial owner.
- Understanding and obtaining information on the purpose and intended nature of the business relationship.
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being

[17] Section 19(1)(e) of the AMLCFT Act
[18] See Chapter 5-New Financial Products And Services As An Emerging ML/TF Threat

conducted are consistent with the business and risk profile of the customer, including, where necessary, the source of wealth and source of funds.

When designing CDD procedures and conducting CDD on customers, reporting entities should, where appropriate, consider the following issues:

- **Purpose and intended nature of business:** A reporting entity should ensure it has a clear understanding of expected activity to support ongoing transaction monitoring. Typically, the key consideration is being able to identify whether the customer's activity (e.g. transaction type, size or frequency) is in line with the reporting entity's knowledge of the customer. Understanding the nature of the business relationship includes understanding any other parties involved within the relationship. This includes verifying the authorisation of persons purporting to act on behalf of the customer, their identification and verification on a risk-sensitive basis and understanding the role the reporting entity plays. In higher risk situations, obtaining further information for ongoing monitoring of the business relationship and detection of potentially suspicious activity may be needed.

- **Beneficial ownership structures:** Where a customer appears to have a less transparent beneficial ownership or control structure, including the presence of corporate vehicles, nominees or private legal arrangements, a reporting entity should ensure to undertake reasonable steps to verify the identity of beneficial owner(s). Reporting entities should also consider whether the opacity of the ownership structure or the identity of one or more beneficial owners is an indicator of elevated risk and whether it is a cause or not for not performing the transaction or terminating the business relationship and considering making a suspicious transaction report.

- **Source of wealth and funds:** Under a Risk Based Approach, a reporting entity should take reasonable measures to establish the source of wealth and source of funds of relevant parties.

In addition, reporting entities should take measures to comply with national and international sanctions legislation; sanction screening is mandatory and is not discretionary.

As a general rule, reporting entities must apply CDD measures to all customers. The extent of these measures may be adjusted, to the extent permitted or required by regulatory requirements, in line with the ML/TF risk associated with the individual business relationship. This means that the amount and type of information obtained, and the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher or decreased where the associated risk is lower.

Reporting entities should conduct CDD on an initial and ongoing basis and should endeavour to be aware of material changes to the customer's legal form, beneficial ownership and nature of business.

A reporting entity should implement procedures to periodically review the customer relationship and CDD Information. The risk based periodic review process should be based on a formal cycle, and additional reviews should be performed based on "trigger event" causes.

Guidance for implementing CDD:

Identifying and verifying the identity of Natural Persons

To identify a customer that is a natural person, the following information must be obtained from the customer:

- Customer's full name
- Permanent and mailing address (including PO Box numbers-if necessary)
- Telephone Numbers, Email etc.
- Date and place of birth - Nationality
- Occupation/or nature of business (where self-employed)
- Name and address of employer (if applicable)
- Signature

To verify the identity of a customer that is a natural person.

Obtain copy of identification document such as –

- National Identification Card,
- Passport or
- Driver's Licence.

Identifying and verifying the identity of Legal Persons

To identify a customer that is a legal person e.g., body corporate/company, foundation, partnership, etc., the reporting entity must at a minimum obtain the following:

- The customer's name, and legal form (e.g. ABC Inc., or ABC Establishment);
- The powers that regulate and bind the legal person (e.g. the articles of incorporation of a company),
- The names and addresses of the relevant persons having senior management position in the legal person (e.g. Director, Chief Executive Officer etc.)
- The address of the registered office, and, if different, a principal place of business.
- Identify and verify the beneficial owners of the legal person, who should be natural persons (eg. Share Register, Resolution, Share Certificate)

To verify the identity of a customer that is a legal person the reporting entity must obtain copy of reliable and independent source documents such as –

- Proof of incorporation or similar evidence of establishment or existence (e.g. Certificate of Incorporation, Partnership Agreement, Certificate of Good Standing or any other documentation from a reliable independent source that can prove the name, form and current existence of the customer).

Identifying and verifying the identity of Legal Arrangements

To identify a customer that is a legal arrangement e.g. trust or other similar type of arrangements, the reporting entity must at a minimum obtain the following:

- The powers that regulate and bind the legal arrangement (e.g. Statement of Trustees, Trust Deed)
- The names and addresses of customer's controlling bodies (e.g. Trustee(s)).
- The address of the registered, and if different, a principal place of business

- Identify and verify the beneficial owner of the arrangement, who should be natural persons

To verify the identity of a customer that is a legal arrangement the reporting entity must obtain a copy of :

- Deed of Trust, or any other documentation from a reliable independent source that can prove the name, form and current existence of the customer.

Identifying and verifying the identity of other types of customers e.g. Government organization or ministry/statutory body. To identify a customer that is a government organization or ministry or statutory body, the following information must be obtained from the customer:

- The name and address of the government organization/ministry/statutory body
- The identification document of the person appearing on behalf of the government organization/ministry/statutory body
- -The authorization permitting/authorizing that person to appear on behalf of the government/organization/ministry/statutory body and powers granted and/or delegated to that person.

To verify the identity of a customer that is a government organization, ministry, or statutory body, the reporting entity must obtain the following:

- a letter from the government organization/ministry/statutory body authorizing the person to appear on its behalf.

Such letter must be on the organization/ministry/statutory body official letterhead; it must carry the official stamp/seal of the organization/ministry/statutory body; and it must be signed by a senior official e.g. Permanent Secretary/Chairman/Director/Chief Executive Officer of the organization/ministry/statutory body.

Identifying the beneficial owner

To identify a customer that is the beneficial owner of a legal person or arrangement (company/partnership etc.):

- Identify the natural person(s) who ultimately have a controlling ownership interest in a legal person or arrangement.

If there is doubt as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, identify the natural person(s) (if any) exercising control of the legal person through other means. Where no natural person is identified, the reporting entity should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

To identify a customer that is the beneficial owner of a legal arrangement such as trust, the following should be obtained:

- the identity of the settlor,
- the identity of the trustee(s),

- the identity of the beneficiaries or class of beneficiaries, and
- the identity of any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership).

For other types of legal arrangements – identify the person(s) in equivalent or similar positions.

When to conduct standard CDD?

The reporting entity must determine its customer's identity using standard CDD measures when -

a) The customer[19] wishes to establish a business relationship[20] with a reporting entity;
b) The customer wishes to conduct a transaction equal to or above the designated threshold specified for the reporting entity under the AML/CFT legislation or as may be prescribed by the Minister of Finance; (c) There is a suspicion that the transaction may be linked to money laundering or terrorist financing;
c) There are doubts about the accuracy or adequacy of previously obtained customer identification data; (e) Completing a transaction for an occasional customer
d) Completing a transaction for a high-risk customer, for example, non- resident customer, Politically Exposed person etc.

NOTE: Section 9 of the AMLCFT Amendment Act No. 1of 2015 which amended Section 15(2A) of the AMLCFT Act provides that if a reporting entity is unable to:

a) verify the identity of a customer, or
b) obtain enough information about the nature or purpose of a transaction,

The following applies:

- In the case of a one-off transaction, the reporting entity must not carry out the transaction for that customer or from entering into a business relationship with the customer.
- Any business relationship already established must be terminated and;
- The reporting entity should submit a Suspicious Transaction Report (STR) to the FIU.

NON- FACE- TO-FACE CUSTOMER

Section 15 (7A) (a) of the AMLCFT Act as amended by **Amendment Acts No. 1 of 2015 and No. 15 of 2016**, provides that a reporting entity shall establish in writing and maintain policies and procedures to address the specific risks associated with non-face-to-face business relationships or transactions, when establishing customer relationships and conducting ongoing due diligence.

Section 15(7A) (b) provides that a reporting entity shall also establish in writing and maintain measures to manage the specific risks including specific and effective customer due diligence procedures that apply to non-face-to-face customers.

[19] Customers include persons, whether natural, legal or legal arrangement

[20] Business relationship means any arrangement between any person and a reporting entity, the purpose of which is to facilitate the carrying out of financial and other related transactions on a regular basis.

If conducting a non-face-to-face business transaction with customer the reporting entity must have policies, procedures, systems and controls in place to manage specific risks associated with such non face-to-face business relationships or transactions.

The reporting entity, at a minimum, must require one form of official identification which has been authenticated (certified appropriately) and one form of documentation that will verify the physical address of the customer.

Where the customer is a legal person, the reporting entity must require documentary evidence of the continuing existence of the legal person's good standing and a certified copy of acceptable identification and address to verify the address of the legal person.

The reporting entity must ensure that adequate procedures for monitoring the activity of non-face to face transactions are implemented and managed effectively.

NON-RESIDENT/FOREIGN CUSTOMER

The reporting entity must pay attention to non-resident/foreign customers[21] (whether natural or legal persons). The same identification requirements for natural persons resident in Guyana also apply to natural person's resident outside of Guyana.

Where certified copies of documents are being used to conduct transactions, the reporting entity must be satisfied that the documents are authentic and that they are the same on all the identification documents presented.

The reporting entity must obtain the reasons for the transaction by the non-resident customer. Where the customer is a foreign company, the same documents required for locally incorporated companies should be requested and retained.

RELIANCE ON THIRD PARTIES/INTRODUCERS

Section 15(8) of the AMLCFT Act as amended by Section 9 of AMLCFT Amendment Act No. 1 of 2015, provides that where a reporting entity relies on an intermediary or third party to undertake its obligations under **subsection (2), (3) or (4)** or to introduce business to it, it shall-

(a) Immediately obtain the information and documents required by subsections (2), (3), and (4);
(b) Take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to customer due diligence requirements will be made available from the third party upon request without delay;
(c) Satisfy itself that the third party or intermediary is regulated and supervised in accordance with international recommended best practices in relation to regulation and supervision, powers of supervisors and regulation and supervision of Designated Non-Financial Businesses and Professions and has measures in place to comply with customer due diligence requirements set out in international recommended best practices in relation to a terrorist financing offence and customer due diligence and record keeping, and in any event the ultimate responsibility for customer

[21] Section 15 applies in conjunction with Section 18(1) of the AMLCFT Act as amended.

identification and verification shall remain with the reporting entity including where it seeks to rely on the third party.

A third party or introducer is an entity which introduces a customer to the reporting entity- a financial institution or DNFBP that is supervised or monitored for, and has measures in place for compliance with, CDD and Record Keeping requirements in line with **FATF Recommendations 10 and 11**.

A reporting entity is permitted to rely on a third party/introducer to undertake its CDD obligations in certain circumstances. If relying on a third party/introducer, the reporting entity must be satisfied that the third party/introducer —

(i) is regulated and supervised for AML/CFT purposes by a supervisory authority or by an equivalent regulatory or governmental authority, body or agency in Guyana or the jurisdiction in which he/she operates or in the case of a company, where it is registered or licensed to operate;

(ii) is subject to the AML/CFT Law or to equivalent legislation of another jurisdiction;

(iii) is licensed, registered, incorporated or otherwise established, whether in Guyana or a foreign jurisdiction that has an effective AML/CFT regime; and

(iv) is not subject to any secrecy or other law or circumstances that would prevent the reporting entity from obtaining any information or original documentation about the customer that the reporting entity may need for AML/CFT purposes.

When reliance is appropriate, after consideration of the above, the ultimate responsibility for CDD remains with the reporting entity - in other words, the reporting entity can delegate the task but not the responsibility. In such situations, the reporting entity should verify that the third party is conducting checks similar to or at a higher level than the reporting entity's own internal standards.

The reporting entity should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in FATF Recommendation 10, and also take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available by the relied upon institution upon request and without delay.

The Reporting entity must, in addition to the above, obtain the third party's full CDD Records which must include at a minimum the customer's –

- **Name**
- **Address**
- **Date of Birth**
- **Principal business or Occupation**
- **Relationship with the third party**

CORRESPONDENT BANKING REQUIREMENTS

Section 15(7) of the AMLCFT Act 2009 as amended by AMLCFT Amendment Act. No. 1 of 2015, provides that a bank or a financial institution shall in relation to its cross-border correspondent banking and other similar relationships:

(i) adequately identify and verify the person or entity with whom it conducts such a business relationship
(ii) Gather sufficient information about the nature of the business of the person or entity
(iii) Determine from publicly available information the reputation of the person or entity and the quality of supervision to which the person or entity is subject to, including whether the person or entity has been subject to a money laundering or terrorist financing investigation or regulatory action;
(iv) Assess the person's or entity's anti-money laundering and terrorist financing controls and ascertain for themselves that such controls are adequate and effective
(v) Obtain approval from senior management before establishing a new correspondent relationship;
(vi) Document the responsibilities of the financial institution and the person or entity; and
(vii) Satisfy itself that a respondent financial institution in a foreign country does not permit its accounts to be used by shell banks.

A typical cross-border correspondent relationship in the securities sector is a relationship between the reporting entity (correspondent), with an intermediary (respondent), which is regulated and supervised by a supervisory authority, for securities transactions.

In such cases, the customer of the respondent would not be considered as a customer of the correspondent, and the FATF Recommendations do not require the correspondent reporting entities to conduct CDD on the customers of their respondent institutions.

One example of these types of relationships could be between a global securities firm (correspondent) executing securities transactions on a stock exchange for a cross-border intermediary, acting as a respondent for its underlying local customers, subject to complying with FATF Recommendation 13 requirements.

KNOW YOUR EMPLOYEE (KYE)[22]

A Know Your Employee (KYE) program means that the reporting entity has a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity.

Policies, procedures, internal controls, job descriptions, codes of conduct and ethics, levels of authority, compliance with personnel laws and regulations, accountability, monitoring, dual control and other deterrents should be firmly in place.

[22] Section 19(1)(b)(vi) and (vii) of the AMLCFT Act, as amended.

Background screening of prospective and current employees, especially for criminal history, is essential to keeping out unwanted employees and identifying those to be removed.

Background screening can be an effective risk-management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record.

Used effectively, the pre-employment background checks may: reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. A reporting entity should also verify that contractors are subject to screening procedures similar to its own.

Red Flags regarding employee behavioral changes:

- Sudden and significant changes in their standard of living.
- Lifestyle and spending habits that aren't consistent with their salary, financial position or level of indebtedness.
- If employee refuses to take time off for no apparent reason.
- Employees who don't allow other colleagues to assist certain customers.
- If employee suspiciously receives gifts or gratuities on a regular basis.
- Employees who are reluctant to accept any promotions or changes in their activities.
- Employees who stay at the office after working hours or that go to the office at odd times for no reasonable explanation

ENHANCED DUE DILIGENCE (EDD)[23]

In addition to standard CDD, reporting entities should examine, as far as reasonable possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transaction, which have no apparent economic or lawful purpose.

If standard CDD inquiry leads to a high-risk determination the reporting entity must conduct enhanced CDD measures, consistent with the risks identified.

The extent of CDD measures may be adjusted, to the extent permitted by applicable regulatory requirements, in line with the ML/TF risk. This means that the amount or type of information obtained, or the extent to which this information is verified, must be enhanced where the risk associated with the business relationship is higher. The type of enhanced due diligence measures applied should be effective and proportionate to the risks. It may also be reduced where the risk associated with the business

[23] Section 16(6) and (7) of the AMLCFT Act, as amended by Amendment No. 1 of 2015.

relationship is lower. Ongoing monitoring can also lead to a reassessment of the customer's risk profile, and should inform whether additional CDD or EDD is required.

Examples of Enhanced Due Diligence and Simplified Due Diligence Measures

Enhanced Due Diligence

- Obtaining additional customer information, such as the customer's reputation and background from a wider variety of sources before the establishment of the business relationship and using the information to inform the customer risk profile.
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the customer risk profile
- Carrying out additional searches focused on financial crime risk indicator (i.e. negative news screening) to better assess the customer risk profile
- Obtaining additional or more particular information about the intermediary's underlying customer base and its AML/CFT controls
- Undertaking further verification procedures on the customer or beneficial owner to better understand the risk that the customer or beneficial owner may be involved in criminal activity
- Obtaining additional information about the customer's source of wealth or the source of funds involved in the transaction
- Verifying the source of funds or wealth involved in the transaction or business relationship to seek to ensure they do not constitute the proceeds of crime
- Evaluating the information provided with regard to the destination of funds and the reasons for the transaction
- Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship
- Requiring that the redemption payment is made through the initial account used for investment or an account in the sole or joint name of the customer
- Increasing the frequency and intensity of transaction monitoring.

Examples of Simplified Due Diligence

Simplified Due Diligence

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer pieces of customer identification data
- Altering the type of verification carried out on customer's identity.

- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established, without collecting additional information or carrying out additional measures related to understanding the nature and purpose.
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if transaction or account values rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates if the securities provider implements or is required to implement a periodic review process based on a formal cycle.
- Reducing the degree and extent of on-going monitoring and scrutiny of transactions, for example based on a reasonable **monetary threshold**

When to conduct EDD?

For higher risk business relationships, a reporting entity must obtain:

Additional information on the customer (e.g. volume of assets, information available through public databases, internet etc., and updating more regularly the identification data of customer and beneficial owner.

- Additional information on the intended nature of the business relationship.
- Information on the source of funds or source of wealth of the customer.
- Information on the reason or intended of performed transactions.
- The approval of senior management to commence or continue the business relationship.

Examples of potentially higher-risk situations include:

- Customers that are Politically Exposed Persons.
- Non-resident customers.
- Legal persons or arrangements that are personal asset-holding vehicles
- Companies that have nominee shareholders.
- Cash intensive businesses.
- Companies with unusual or excessively complex ownership structure.
- Customer in countries with inadequate AML/CFT systems. Customer in countries subject to sanctions, embargos or similar measures issued by reputable international organisations e.g. FATF/UN
- Non-face-to-face business relationships or transactions.
- Correspondent banking relationships.
- Money and wire transfer services

Politically Exposed Persons[24]

[24] Section 15(4)(d) and (e) of the AMLCFT Act as amended by Amendment No. 1 of 2015.

A Political Exposed Person (PEP) is any individual who is or has been entrusted with prominent public functions on behalf of a State, including –

- A Head of State or of government;
- Senior politicians, - Senior government, judicial or military officials,
- Senior executives of State-owned corporations,
- Important political party officials, including family members or close associates of the PEP whether that person is resident in Guyana or not.

Since PEPs are considered higher-risk customers, reporting entities must take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP, a person who is or has been entrusted with a prominent function by an international organization or by a foreign country (international organization PEP or Foreign PEP respectively).

When dealing with a customer or beneficial owner who is a PEP, the reporting entity shall:-

- The reporting entity must adequately identify and verify the person's identity by obtaining the information required to identify and verify the identity of the natural person(s) who is the PEP
- Have appropriate risk management systems to determine whether a customer or beneficial owner is a PEP;
- Obtain the approval of senior management before establishing a business relationship with a PEP,
- Take reasonable measures to establish the source of wealth and source of property, and
- Conduct regular enhanced monitoring of the business relationship,
- If a customer is subsequently found or becomes a PEP, the reporting entity shall require its senior management to approve the continuation of the business relation with such a person.

RECORD KEEPING

Section 16 of the AMLCFT Act 2009 as amended requires that reporting entities maintain all records of its customer's transaction for **at least seven (7) years** from the date the relevant transaction was completed, or termination of business relationship, whichever is later.

Reporting entities must maintain, all records on transactions, both domestic and international, to enable them to comply swiftly with information requests from competent authorities, e.g., FIU, the Special Organised Crime Unit (SOCU), Supervisory Authorities (SA)

Guidance for Record keeping:

The reporting entity must keep records to provide sufficient information on the business relationship with the customer as follows:

- Records of the evidence of the customer's identity (eg. Copies or Records of official identification documents like passports, ID cards, driving licences

- Records of account files and business correspondence in relation to transactions and identities of persons involved in the transactions (Eg. Inquiries to establish the background and purpose of complex, unusual large transactions)
- The name, date of birth, address and occupation of the customer, and where appropriate, the business or principal activity of each person conducting the transaction, on whose behalf the transaction is being conducted, as well as the method used by the reporting entity to verify the identity of each person;
- Records of the type and amount of currency involved in the transaction (e.g. the reporting entity must record, the type of currency - whether, United States dollar, Canadian dollar, Guyana dollar, etc., and also include, whether it is coin, paper money, bank notes or other negotiable instruments), including whether any other individuals or entities were involved in the transaction.
- Records of the nature and date of the transaction.

Maintenance of Records: A reporting entity must ensure that there is in place, an effective storage system that will facilitate the protection of documents. That is to prevent records from becoming, blurred, defaced, illegible, mutilated or in any other way deteriorated. Where records are being stored digitally or electronically, they must be easily retrievable or capable of reproduction in a printable and legible (readable) form.

Records Retrieval: Records must be retrieved promptly or without undue delay by the reporting entity. In other words, upon request for information by the FIU or other authorised authority, the reporting entity must ensure that the information is submitted (promptly) by the date specified by the requesting authority; or an order of the court.

Other record keeping functions: In addition to records of its customer's transactions, a reporting entity must also keep –

- a special register for AMLCFT enquires; and
- records of customer risk profiles.

The register of AMLCFT enquires must contain at a minimum:

- the date and nature of the enquiry;
- the name and agency of the inquiring officer;
- the powers being exercised and
- details of the accounts or transaction involved.

Records must be kept up to date and reviewed on an ongoing basis. Also, the reporting entity should establish safeguards for records, that is, a place for storage of back up, information offsite or onsite or other as may be determined by the reporting entity.

Records must be kept and maintained for at least seven (7) years from the date the relevant transaction was completed, or termination date of business relationship, whichever is the later.

REPORTING[25]

Reporting entities are required to submit three (3) types of reports to the FIU in such manner and form as specified by the Director of the FIU. These reports are as follows:

[25] Information for this part - 'Reporting' was extracted from FIU's AMLCFT Handbook for Reporting Entities published on 18th February, 2021.

- Threshold Transaction Report
- Suspicious Transaction Report
- Terrorist Property Report

THRESHOLD TRANSACTIONS REPORTS (TTRS)

TTRs are reports of transactions conducted by customers of reporting entities that meet pre-determined limits/thresholds, as may be specified in the law or stipulated by the FIU. Any cash, and in some specific non-cash instances, transactions facilitated by reporting entities for a customer, single or accumulated, within a specified period, usually a month, that meets the following threshold are required to be reported to the FIU. For Financial institutions as defined in the **Fourth Schedule of the AMLCFT Act**.

Reporting Entities within the Financial Sector	**Reporting Threshold**
Commercial Banks	Any cash transaction amount to in single or accumulation **GY$2,000,000 (two million dollars) and above**
Insurance companies and brokers	Any cash transaction amount to in single or accumulation **GY$2,000,000 (two million dollars) and above**
Securities companies and brokers	Any cash transaction amount to in single or accumulation **GY$2,000,000 (two million dollars) and above**

TTRs are due by the 7th day of each month, following the month in which the transaction(s) occurred and should be reported in such a manner and format as prescribed by the Director of the FIU[26].

SUSPICIOUS TRANSACTION REPORTS (STRS)

A STR is a report which reporting entities are required to submit to the FIU, whenever there is a suspicion or reasonable grounds to suspect that funds or a transaction (attempted or completed or on-going), are connected to the proceeds of a criminal activity, money laundering, terrorism, or terrorist financing or proliferation financing.

Section 18(4) of the AMLCFT Act, as amended provides reporting entities to:

a) Take reasonable measures to ascertain the purpose of the transaction, the origin and ultimate destination of the funds involved and the identity and address, of any ultimate beneficiary, and
b) Prepare a report of the transaction in accordance with subsection (8) and send the report to the FIU in such other form as the Director may approve.

[26] https://fiu.gov.gy/essential-forms/

Section 18(8) of the AMLCFT Act, as amended, provides that a report required under subsection (4) above, shall –

a) Contain particulars of the matters specified in **subsection (4)(a) above and Section** 16;

b) Contain a statement of the grounds on which the reporting entity holds the suspicion, and

c) Be signed or otherwise authenticated by the reporting entity.

As a general principle, any transaction that causes a reporting entity to have an apprehension or mistrust, should be considered for submission to the FIU as a suspicious transaction.

Guidance for suspicious transaction reporting[27]

Identifying suspicious transaction

Suspicious transactions are likely to involve a number of factors which together raise a suspicion in the mind of the officer of the reporting entity that the transaction may be connected to money laundering, terrorist financing or the proceeds of a crime.

The factors that should be considered in assessing whether or not a transaction is suspicious include - complex, unusual large business transactions, and unusual patterns of transactions, whether completed or not, that have no apparent economic or lawful purpose and are inconsistent with the profiles of the person or persons carrying out the transactions.

Reporting entities can seek guidance as to what could constitute an STR from the list of indicators provided in the Annex.

Note that this list of indicators is for guidance only.

Further guidance may be obtained from typologies and case studies provided in the typology reports produced and circulated by the FIU.

What is a suspicious transaction? This will ultimately be determined by the reporting entity's knowledge of its customers, their business and historical pattern of transactions.

What to report?

An STR submitted to FIU must contain:

a. Information on the subject (Name/DOB/Occupation) including copy of ID if available.
b. Information related to the suspicious activity (Date range of suspicious activity/Account details/type of transaction/Amount involved).
c. Information on the reporting entity making report (Name and address of reporting entity).
d. Information on Compliance Officer of the reporting entity (Name and contact details of the Compliance Officer).

[27] See FIU Handbook for Reporting Entities page 32

e. A description of the suspicious transaction/activity: Provide a clear, complete and chronological description of the transaction(s), including what is unusual, irregular, or suspicious about the transaction(s), using the checklist below as a guide:

Describe

(i) The conduct that raised suspicion; and
(ii) The supporting documentation.

Explain

(i) Whether the transaction(s) was completed or only attempted; and
(ii) Who benefited, financially or otherwise, from the transaction(s).

Indicate

(i) Whether any information has been excluded from this report and why;
(ii) Whether the suspicious transaction is an isolated incident or relates to another transaction; and
(iii) If the reporting entity is a financial institution) any additional account number and any domestic or foreign bank account number which may be involved.

When to report?

Once a suspicion is formed, a reporting entity must as soon as practicable, but no later than three days after forming a suspicion, report the transaction to the FIU. In practice, where account monitoring processes identify a transaction, the **three-day requirement does not commence until a suspicion based on reasonable grounds is formed**. Reasonable grounds may not exist until a member of your staff has had time to consider the transaction in light of the surrounding circumstances or new information is obtained. Once the requisite suspicion is formed, the **three-day requirement** commences.

After an initial STR has been submitted, a reporting entity may continue to conduct business with the customer. However, they must comply with all relevant provisions of the AML/CFT legislation, including the requirement to submit additional information on the customer where appropriate.

IMPORTANT: The requirement to report STRs applies to completed or attempted transactions and there are no monetary thresholds for reporting.

FATF Recommendation 10 requires in cases where financial institutions form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process, and instead should be required to file an STR.

TERRORIST PROPERTY REPORTS (TPRS)

A TPR is a report that a reporting entity must submit to the FIU, whenever it has knowledge that funds or other assets in its possession are for a person or entity that is listed on the United Nations Security Council (UNSC) Consolidated list or listed or specified by order of the Minister of Finance, in accordance with **Section 2(2) of the AMLCFT Act, 2009, and UNSCR 1373 (2001)**.

A TPR must be submitted immediately (without delay) after the person (legal or natural) has been identified as having such association.

Guidance for terrorist property reporting[28]

To determine whether you are in possession of funds or other assets of a listed person or entity, you must first determine whether any of your customer/client is a listed person or entity, and also whether you are dealing with any funds or other assets of that listed person or entity.

Positive name match relating to listings by the Al Qaida 1267(1999) Sanctions Committee or the 1718(2006)/2231(2015) (on DPRK and Iran) Sanctions Committees or Minister of Finance in accordance with UNSCR 1373.

If there is a '**positive name match**' meaning that the name of the customer/client appears on the **UN Consolidated List (UNSCRs 1267, 1718 and 2231), or Local List (UNSCR 1373)**, a reporting entity must:

(i) Take reasonable and appropriate measures to verify and confirm that the customer/client is the listed person or entity before informing the Director-FIU.

This can be done by further checking, in the case of a person, the customer/client's date of birth, place of birth, nationality, and ID Card/Passport number, and in the case of an entity, the entity's address and other information, against the information on the UN Consolidated List or Local List. (This will avoid false positive situation where extreme measures may be taken against an innocent person or entity)
AND

(ii) If customer/client's details match, immediately complete and submit a Terrorist Property Report.

(iii) If the reporting entity is in possession or control of any funds or other assets of the listed person or entity the following information must also be included in the report:
   a. Number of persons
   b. Contracts or accounts involved
   c. Total value of the funds or other assets.

Terrorist Property Quarterly Report
A reporting entity is also required to submit Quarterly Terrorist Property Report to the FIU whether or not it had dealings with a listed person or entity. 17 Such reports are due as follows:

- **On or before January 7 – for the quarter (October – December)**
- **On or before April 7 - for the quarter (January – March)**
- **On or before July 7 – for the quarter (April – June)**
- **On or before October 7 – for the quarter (July – September)**

NOTE:
While the **UN Consolidated list contains listings by the Al Qaida 1267(1999) Sanctions Committee or the 1718(2006)/2231(2015) (on DPRK and Iran) Sanctions Committees**, it is important to note that the list also contains listings by other Sanctions Committees such as the Sanctions Committee concerning Iraq, the 2127 Committee concerning Central Africa, and the 2374 Sanctions Committee.

[28] See FIU Handbook for Reporting Entities page 33

Positive name match relating to listings by other Sanctions Committees

If there is a 'positive name match' a reporting entity must:

(i) Take reasonable and appropriate measures to verify and confirm that the customer/client is the listed person or entity before informing the Director-FIU; and

If customer/client's details match, immediately complete and submit a Suspicious Transaction Report to the FIU.

Maintaining sanctions lists

To determine whether you are in possession or control of funds or other assets of a listed person or entity, you must put in place and implement policies and procedures to-

(a) Keep your entity updated with the various resolutions passed by the United Nation Security Council on targeted financial sanctions related to terrorism, terrorism financing and proliferation financing (UN Consolidated List), as well as Specified Orders passed by the Minister of Finance (Local List); and

(b) Maintain an updated and current database of names and particulars of persons or entities designated by the United Nations Security Council Sanctions Committee (UN Consolidated List) or specified by the Minister of Finance (Specified Order List).

The UN Consolidated List can be accessed on:
https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/consolidated.xsl

OR via the FIU's website at https://fiu.gov.gy

Targeted Financial Sanctions (Specified Person/Entity) Order referred to as the "Local List" can be accessed at: https://fiu.gov.gy

Conduct screening on customers

A reporting entity must conduct checks on its existing, new and potential customers/clients, via a name-screening and/or internal blacklist database to determine if a customer/client is listed on the UN Consolidated List or the Local List.

A reporting entity must screen its entire customer/client database without delay when informed of new names added to the UN Consolidated List or Local List.

The obligation to conduct screening on customers/clients also includes funds or other assets derived from property owned or controlled directly or indirectly by the listed person or entity. In this regard a reporting entity must conduct checks on-

(a) Relationship and transactions connected with the listed person or entity.
(b) Properties or accounts that are jointly owned and/or indirectly controlled by the listed person or entity; and
(c) Parties related to the accounts including beneficial owners, signatories, power of attorney relationships, guarantors, nominees, trustees, assignees and payors.

CHAPTER 4 - LIABILITY, SANCTIONS & INFORMATION SHARING

NO LIABILITY FOR INFORMATION & TIPPING OFF

NO CRIMINAL OR CIVIL LIABILITY FOR INFORMATION

Section 11(1) of the AMLCFT Act, as amended, provides that no proceedings for breach of professional confidentiality may be instituted against any person or against directors, officers or employees of a reporting entity, who in good faith transmits or submits suspicious transactions, or suspicious activity reports to the FIU, in accordance with the AMLCFT Act, even if the person, director, officer or employee did not know precisely what the underlying criminal activity was, and regardless of whether the illegal activity actually occurred.

There is no criminal or civil liability to a person who submits an STR or submit any related information to the FIU in relation to ML/TF/PF.

Section 11(2) of the AMLCFT Act, as amended, provides that there is NO civil or criminal liability action may be brought nor may any professional sanction be taken against any person or agent of any reporting entity for breach of any restriction on disclosure who in good faith transmits information or submits reports to the FIU.

TIPPING OFF

Section 5 of the AMLCFT Act, as amended, provides that it is an offence for a person who knows or suspects that a suspicious transaction report or related information is reported to the FIU, or that an investigation into money laundering, terrorist financing, or the proceeds of crime has been, is being or is about to be made, to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

IT IS AN OFFENCE TO TIP OFF
A person commits an offence under Section 5(1) above and is liable to summary conviction to a fine of one million dollars (GY$1,000,000) and to imprisonment for three (3) years.

FATF Recommendation 10 requires in cases where financial institutions form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should be permitted not to pursue the CDD process, and instead should be required to file an STR with the Financial Intelligence Unit.

SANCTIONS

Supervisory Authorities may impose administrative or criminal sanctions against Reporting Entities for Non-Compliance of its obligations under the AMLCFT legislation.

Administrative Sanctions

Supervisory Authorities can impose one or more administrative sanctions against a reporting entity that fails, neglects or refuses to comply with its obligations under the AMLCFT legislation.

These sanctions are set out in **Section 23(1) of the AMLCFT Act, as amended** and includes:

- Written warnings,
- Order to comply with specific instructions,
- Order regular reports from the reporting entity on measures it is taking,
- Prohibit convicted person(s) from employment with the reporting entity,
- Recommend to the appropriate licensing authority of the reporting entity (where the supervisory authority is not the regulator) that the reporting entity's license/registration be suspended, restricted or withdrawn,
- Removal of defaulting director or senior manager from the Board or relieve him/her from the functions related to the default, and/or
- Impose a fine against the reporting entity of no less than five million dollars (GY$5,000,000) and no more than fifteen million dollars (GY$15,000,000).

Criminal Sanctions

Section 23(2) of the AMLCFT Act, as amended, provides that a reporting entity or any of its directors, managers, officers or employees, that breaches its obligations under the AMLCFT legislation can be criminally sanctioned.

In the case of a breach of an individual, the penalty is a fine of no less than five million dollars (GY$5,000,000) and no more than fifteen million dollars (GY$15,000,000), **and** imprisonment to a minimum of three (3) years.

In the case of a breach of a company/body corporate, the penalty is a fine of no less than fifteen million dollars (GY$15,000,000) to a maximum of forty million dollars (GY$40,000,000).

SHARING OF INFORMATION & FINANCIAL INSTITUTIONS' SECRECY LAWS[29]

Section 111 of the AMLCFT Act, **as amended**, provides that subject to the provisions of the Constitution, the provisions of the AMLCFT Act shall have the effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by any law or otherwise.

Section 112 of the AMLCFT Act further provides that it shall not be unlawful for any person to make any disclosure in compliance with the AMLCFT Act.

Section 17 of the Bank of Guyana Act No. 19 of 1998 provides that any information obtained under the **Bank of Guyana Act** shall be confidential and shall be used by the Bank solely for the performance of its

[29] Recommendation 9 of FATF Recommendations

functions under this Act, **save and except**, for the purpose of the performance of his duties or the exercise of his functions, or when lawfully required to do so by any Court or **under the provisions of any law.**

Section 19(1) of the Securities Industry Act, 1998 provides for the GSC to consult and cooperate with the Bank of Guyana, or any other agency that exercises regulatory authority under a written law over a financial institution, insurance company or other body in order to minimize duplication of effort and to maximize the protection of investors.

Section 19(3) of the Securities Industry Act, 1998 allows the GSC to cooperate in the work of national, regional or international organizations dealing with the regulation of securities markets. Further, **Section 19(2)** further allows the GSC to cooperate with any agency of a foreign government in connection with an investigation in contravention of the **Securities Industry Act or any similar law**, whether the activities occurred in or outside of Guyana.

Section 3 of Amendment Act No. 12 of 2022 of the AMLCFT Act, **Section 9(4) of the Principal AMLCFT Act** was amended to allow for the sharing of information with law enforcement agencies or investigative authorities, including, information-

- Derived from an inspection carried out by a supervisory authority pursuant to Section 22 of the Act, if it gives the FIU reasonable grounds to suspect that a transaction involves money laundering, proceeds of crime or terrorist financing,
- To a supervisory authority or other competent authority for the purposes relating to investigations or enquires contemplated under the AMLCFT Act, inter alia.

CHAPTER 5 - EMERGING ML/TF/PRF CHALLENGES & THREATS

UNDERSTANDING BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS[30]

Corporate vehicles—such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements—conduct a wide variety of commercial and entrepreneurial activities. However, despite the essential and legitimate role that corporate vehicles play in the global economy, under certain conditions, they have been misused for illicit purposes, including money laundering (ML), bribery and corruption, insider dealings, tax fraud, terrorist financing (TF), and other illegal activities. This is because, for criminals trying to circumvent anti-money laundering (AML) and counter-terrorist financing (CFT) measures, corporate vehicles are an attractive way to disguise and convert the proceeds of crime before introducing them into the financial system.

The misuse of corporate vehicles could be significantly reduced if information regarding both the legal owner and the beneficial owner, the source of the corporate vehicle's assets, and its activities were readily available to the authorities. Legal and beneficial ownership information can assist law enforcement and

[30] See FATF Guidance on Transparency and Beneficial Ownership published October, 2014.

other competent authorities by identifying those natural persons who may be responsible for the underlying activity of concern, or who may have relevant information to further an investigation. This allows the authorities to "follow the money" in financial investigations involving suspect accounts/assets held by corporate vehicles.

In particular, beneficial ownership information can also help locate a given person's assets within a jurisdiction. **FATF Recommendations 24 and 25 outline** the standards on transparency and beneficial ownership of legal persons and arrangements. Adequate, accurate and timely information on beneficial ownership of corporate vehicles must be available and be accessed by the competent authorities in a timely manner.

Reporting Entities should take appropriate measure to prevent the misuse of legal persons for Money Laundering and Terrorist financing, including ensuring information about the beneficial ownership and control of such legal persons is available to competent authorities.

Beneficial Owner: A beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement1. 'Ultimately owns or controls' and 'ultimate effective control' refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

Beneficial Ownership : "Beneficial Ownership" means ownership by a natural person or persons who ultimately exercise individually or jointly voting rights representing **at least twenty-five per cent** of the total shares, or otherwise have ownership rights of a legal entity; or ownership by a natural person or persons who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes those persons who exercise ultimate effective control over a legal person or arrangement; **(AMLCFT (Amendment) Act No. 10 of 2015).**

Pursuant to **Section 3(1)(e) of the Securities Industry Act 1998**, beneficial ownership includes *' ownership through a trustee, legal representative, agent, nominee or other intermediary."*

Ultimate Beneficial Owner or Ultimate Beneficial Ownership, in the context of conducting customer due diligence, always aims at ascertaining the identity of the human being(s) behind the corporate veil or transaction NEVER a legal entity, although obtaining identification and verification information/documentations are necessary for all transactions conducted with the legal person(s).

Beneficiary: The term beneficiary, depending on the context, means a person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural person or legal person/entity. The term beneficiary also applies in the context of a 'Beneficiary Financial Institution', when it carries out transactions relating to cross border and/or domestic wire transfers. The FATF Definition of beneficial ownership from the Glossary to the FATF Recommendations is *'Beneficial owner refers to the natural person(s) who ultimately[31] owns or controls a customer[32] and/or the natural person on whose behalf a*

[31] Reference to 'ultimately owns or controls' and 'ultimate effective control' refers to situation in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.
[32] This definition should also apply to beneficial owner or a beneficiary under a life or other investment linked insurance policy.

transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement."

Express Trust: Express trust refers to a trust clearly created by the Settlor, usually in the form of a document, example, a written Deed of Trust. They must be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a Settlor to create a trust or similar arrangement, example resulting or implied trust.

Legal Arrangement: Legal arrangements refer to express trusts or other similar legal arrangements. The FATF definition of beneficial owner also applies in the context of legal arrangements, meaning the natural person(s), at the end of the chain, who ultimately owns or controls the legal arrangement, including those persons who exercise ultimate effective control over the legal arrangement, and/or the natural person(s) on whose behalf a transaction is being conducted. However, in this context, the specific characteristics of legal arrangements make it more complicated to identify the beneficial owner(s) in practice.

Legal Persons: A legal person refers to 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, association, partnerships or other relevantly similar body. An essential element of the FATF definition of beneficial owner is that it extends beyond legal ownership and control to consider the notion of ultimate (actual) ownership and control. In other words, the FATF definition focuses on the natural (not legal) persons who actually own and take advantage of capital or assets of the legal person; as well as on those who really exert effective control over it (whether or not they occupy formal positions within that legal person), rather than just the (natural or legal) persons who are legally (on paper) entitled to do so.

Settlor: A Settlor is a natural or legal person who transfers ownership of his/her/it assets to a trustee(s) by means of a trust deed or similar arrangement

Importance of Obtaining Beneficial Ownership Information

Section 15 of the AMLCFT Act as amended and Regulation 4(5) of the AMLCFT Regulations No. 4 of 2010 requires reporting entities to identify and verify beneficial ownership and control structure of legal entity or legal arrangement when they establish or carry out business transactions with such customers. Additionally, international standards14 require countries to ensure transparency of transactions to deter and prevent the misuse of corporate vehicles for criminal purposes.

It is recognized that many criminal enterprises try to hide the true ultimate owners and effective controllers of illegally obtained assets, through, inter alia, 'shell companies, complex ownership and control structures, trusts and other similar legal arrangements, including the use of intermediaries in forming legal entities. It is sometimes difficult to identify and verify beneficial owner(s) due to the varying ownership structures that may be involved in transactions with the reporting entity.

These structures range from very simple to very complex in nature and can be spread across multiple jurisdictions. It is therefore crucial that reporting entities be alert at all times to recognise or detect the various arrangements or transactions before them, as there may be attempts to conceal proceeds of criminal activities of a beneficial owner through their businesses.

Mechanisms for Obtaining Beneficial Ownership Information

The reporting entity must develop policies and procedures (which may be included in an AML/CFT Compliance Manual) that express clearly the type of information required to be collected when transacting business with the various forms of legal persons or legal arrangements.

One of the primary objectives is to determine those customers who own **at least twenty five percent (25%)** shares in the entity; or who is the natural person or persons who otherwise ultimately owns or controls a customer; or the person on whose behalf a transaction is being conducted, including in all instances to identify those persons who exercise ultimate effective control over the legal person or arrangement. Additionally, the reporting entity must seek to obtain information on the number of shares, the categories of shares, the associated voting rights and whether there is any shareholder's agreement that would indicate any specified dominant influence or power to appoint senior management officials.

The reporting entity should also seek to establish whether any appointees are closely connected to the transactions by their participation in the financing of the legal persons, through family relationships, contractual associations or by defaults on certain payments by the legal entity. A salient element in determining who the senior management officials are is to ascertain whether they are also the ultimate beneficial owners of the legal entity or arrangement or simply just manage the day to day business.

If they simply manage the affairs of the business, the entity must seek to establish the medium/authorisation through which these officials are vested with authority to act in such capacities.

The lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising:

- The Identity of known or suspected criminals
- The true purpose of an account or property held by a corporate vehicle
- The source or use of funds or property associated with a corporate vehicle

Beneficial Ownership Information can be obscured through the use of:

a) Shell Companies (which can be established with various of ownership structure), especially in cases where there is foreign ownership which is spread across jurisdictions.
b) Complex Ownership and control structures involving many layers of shares registered in the name of other legal persons
c) Bearer shares and bearer share warrants
d) Unrestricted use of legal person as directors
e) Formal nominee shareholders and directors where the identity of the nominator is undisclosed.
f) Informal nominee shareholders and directors such as close associates and family, and
g) Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.
h) Use of intermediaries in forming legal persons including professional intermediaries.

Below are some possible questions the reporting entity may ask in order to determine or obtain the relevant information:

a) Who are the individuals having at least 25% voting rights in the company?
b) Who are the individual having effective control of the business/transaction?
c) Who is the customer acting on behalf of?
d) Who owns 25% shares/or investment in the company?
e) Who are the managers/directors (who have direct or indirect control in the structure)?
f) Are the senior managers/directors the owners of the transaction/s?

The individual(s) who fit any of the questions or any combination of them are the customers the reporting entity must seek to know and verify.

As a general rule: 'Once a reporting entity enters into a business relationship with a customer or client who acts on behalf of another person, ALWAYS ascertain the true identity of the natural person(s) on whose behalf a transaction is conducted and who benefits from the transactions.

As a best practice measure, the reporting entity may develop **'standard forms'** for the customer to complete that would allow for the information to be provided to the entity prior to establishing the business relationship**.**

Information Required to be Obtained:

Where the transaction is being conducted by a legal person(entity):

a) The Name of the legal entity/business
b) The registered address of the entity
c) Country of Incorporation of the entity
d) Information on the purpose and intended nature of the Business relationship
e) Identity of Principal owners/shareholders
f) Identity of Directors, Secretary or Partners, including nominee Directors
g) Evidence of the authority given to enter into a business relationship (for e.g. a copy of the Board Resolution)
h) Share Certificate issued by the entity
i) Articles of Incorporation or continuance
j) Certificate of Incorporation or continuance
k) By-Laws or constitution of the entity
l) Partnership Deed-If business is a partnership
m) Business Registration and Operation licences-where necessary
n) Nature of business, purpose of transaction and source or use of funds or property

Where the transaction is being Conducted through a legal arrangement:

a) Identification of the person acting on behalf of someone, the Principal/Settlor/Donor, including the intended beneficiaries of the transaction;

b) Obtain copies of Powers of Attorney (updated, appropriately notarised and duly registered by the Deeds Registry);

c) Obtain document to support authorisation to act on behalf of the customer;

d) Trust Instruments - e.g. Trust Deeds or other similar document.

In the case of financial institutions, when conducting a cross border wire transfer (in which case the term beneficiary applies):

a) The name of the beneficiary;

b) The beneficiary account number where such an account is used to process the transaction;

c) The name of the originator;

d) The originator account number (where such an account is used to process the transactions); and

e) The originator's address, or national identity number, or customer identification number, or date and place of birth.

Where the Beneficial Owner of the transaction is found to be a Politically Exposed Person (PEP), the reporting entity must conduct enhanced due diligence (EDD), including the following:-

Who has Ultimate Effective Control?

The reporting entity must seek to understand the ultimate effective control system as part of the beneficial ownership structure of a transaction. The directors or senior managers of some companies are also the owners and main decisions makers. In such case, they carry both classifications; the ultimate effective controllers and the ultimate beneficial owners. This situation must not be confused with the company law concepts of control by the directors of a company who are not the ultimate owners of the company. In this case, the reporting entity must distinguish ultimate beneficial ownership (on the one hand) and control by management (on the other hand).

Who are the Senior Management Officials?

Senior Management Officials include, but are not limited to, such positions as, Directors or Senior Managers, Chief Executive Officer, Chief Financial Officers, Executive Directors, President or the natural person(s) who has significant authority over the legal person's financial relationship and include a financial institution that hold accounts and ongoing financial affairs on behalf of a legal person. All of the mentioned positions are persons referred to as fiduciaries16; they are in a position of trust, as they must act in the best interest of the legal entity on which behalf they act or represent.

The authority for senior offices to act on behalf of a legal entity is usually expressed in the entity's by-laws, constitutions, trust instruments, business agreement or other similar documents. It must be noted that, although the Directors or Senior Managers may not be the ultimate owners of the business transaction nor have the requisite number of shares or voting rights in the legal entity, they may have a significant controlling authority to legally bind the company or make financial commitments on behalf of the entity for certain transactions.

The reporting entity, in such instances, must ensure supporting evidence to substantiate the acts being carried out to conduct the business transaction. The maintenance of accurate and update records of the information received from any business transaction with such customer(s) must be kept and be accessible upon request by any authority legally permitted to make such request.

NEW FINANCIAL PRODUCTS AND SERVICES AS AN EMERGING ML/TF THREAT

New technologies have the potential to make AML/CFT measures, fast, cheaper and more effective. If utilized correctly, they can advance the AML/CFT efforts, ensure financial inclusion, and reduce financial exclusion. Innovative technologies and business models bring with it the ease of doing business and bolsters the economy. This has the effect of pushing for the 'smart' improvement in the regulation and supervision within the financial sector to address risks and promote responsible innovation.

Financial institutions should identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products: **Recommendation 15 of FATF Recommendations and Section 19(1)(e) of the AMLCFT Act, as amended.**

Financial institutions should conduct risk assessments prior to the launch or use of such products, practices and technologies and taking appropriate measures to manage and mitigate risks.

Like any other product or service, virtual assets (VAs) and virtual asset service providers (VASPs) are a form of new technology within the financial sector and are vulnerable for misuse for ML/TF/PF purposes.

Some risks posed by VAs and VASPs are:

- Potential for greater anonymity and availability of anonymity enhancing features making it difficult or sometimes impossible to detect, track and trace.
- Non-face-to-face activities complicates the adequate identification of customers during the onboarding process and increases the risk of forged or inaccurate identification information.
- Monitoring, prevention and detection of illegal transactions and disguise of origins of funds may become more prevalent in decentralization and fragmentation of financial products and services, making regulation and supervision difficult.
- Significant potential for regulatory arbitrage especially where the AML/CFT preventive framework is in the early stages of implementing the FATF standards.

What are virtual assets (VAs)?

A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered and defined elsewhere (in the FATF Recommendations)[33].

Virtual assets could range from any type of 'crypto asset' or 'cryptocurrency' and includes so called 'stablecoins' or 'global stablecoins (GSCs)'. These VAs rely on the use of 'Distributed Ledger Technology'

[33] Definition taken from FATF Recommendations (2020)

(DLT) which is a database that is stored, shared and synchronized on a computer network. Blockchain technology is a type of distributed ledger technology (DLT).
Some popular examples are:

- Bitcoin
- Ethereum
- Dogecoin
- Non-Fungible Tokens (NFTs)

What are virtual assets service providers (VASPs)?
Virtual asset service provider means any natural or legal person who is not covered elsewhere (under the Recommendations), and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:-

(i) Exchange between virtual assets and fiat currencies
(ii) Exchange between one or more forms of virtual assets
(iii) Transfer of virtual assets
(iv) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, and
(v) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.[34]

Does Guyana permit or prohibit the use of VAs and VASPs?
VAs and VASPs are not regulated or supervised in Guyana and were identified as an emerging ML/TF threat in Guyana's NRA (2019).[35]

The **AMLCFT Act**, as amended, has sought to define '**proceeds of crime'** by expanding the definition through **Amendment No. 1 of 2015** to mean '…and indirect proceeds of crime including income, profits or other benefits from proceeds of crime and property held by any other person and assets of every kind whether tangible or intangible.' Virtual assets by their name and nature are 'intangible' assets.

The **AMLCFT Act**, as amended, has also sought to extend the definition of **'property'** to include 'money, investments, holdings, legal documents, or digital, evidencing title to or interests in assets of every kind, all possessions, assets and all other property moveable or immoveable, tangible, or intangible, including a chose in action and any other property wherever situated whether in Guyana or elsewhere and includes any interest in such property and includes indirect proceeds of crime including income, profits or other benefits from proceeds of crime and property held by any other person and assets of every kind, whether tangible or intangible.'

Based on **Recommendation 15 of the FATF Recommendations**, **Section 19(1)(e) of the AMLCFT Act**, was amended by **Amendment No. 1 of 2015** to cater for new technologies.

It provides that reporting entities shall-
Identify and assess ML/TF risks and take appropriate measures to manage and mitigate those risks which may arise in relation to –

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

[34] Definition taken from FATF Recommendations (2020)
[35] https://fiu.gov.gy/wp-content/uploads/2022/11/FINAL-NRA-Report-August-12-2021.pdf at page 11-12

And this risk assessment shall take place prior to the launch of new products, business practices or the use of new or developing technologies.

Therefore, reporting entities, launching a new financial product or service or business practice, in keeping with the use of new or developing technologies, is required to conduct a risk assessment of the product or service or business practice to be offered. This also includes the delivery mechanisms and for the use of new or developing technologies for new or pre-existing products. Reporting entities are required to identify and assess the risks and take appropriate measures to manage and mitigate these risks.

In so doing, **Section 22(2)(a) of the AMLCFT Act** provides for the GSC, as the supervisory authority, to examine and supervise the reporting entity, and regulate and oversee effective compliance with the obligations set out in **Sections 15, 16, 18, 19, and 20**, and any other preventive measures in relation to combating ML/TF.

LIST OF ANNEXES:

ANNEX A- MONEY LAUDNERING INDICATORS/RED FLAGS

UNUSUAL CUSTOMER BEHAVIOR

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses a financial institution's record-keeping or reporting requirements with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be reported.
- Customer suggests paying a gratuity to an employee.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.
- Customer, who is a public official, opens account in the name of a family member who begins making large deposits not consistent with the known sources of legitimate family income. Customer, who is a student, uncharacteristically transfers or exchanges large sums of money.
- Account shows high velocity in the movement of funds, but maintains low beginning and ending daily balances.
- Transaction involves offshore institutions whose names resemble those of well-known legitimate financial institutions.
- Transaction involves unfamiliar countries or islands that are hard to find on an atlas or map.
- Agent, attorney or financial advisor acts for another person without proper documentation, such as a power of attorney.
- Customer conducts an unusually high level of transactions over the Internet or by telephone.
- Customer purchases a number of open-end prepaid cards for large amounts, inconsistent with normal business activity.
- Funds withdrawn from the accounts are not consistent with the normal business or personal activity of the account holder or include transfers to suspicious international jurisdictions.
- Customer uses a personal account for business purposes.
- Customer repeatedly uses bank or branch locations geographically distant from customer's home or office without sufficient business purpose.

UNUSUAL CUSTOMER IDENTIFICATION CIRCUMSTANCES

- Customer furnishes unusual or suspicious identification documents or declines to produce originals for verification.
- Customer is unwilling to provide personal background information when opening an account.
- Customer tries to open an account without identification, references or complete local address.
- Customer's permanent address is outside of the institution's service area.
- Customer's home or business telephone is disconnected.
- Customer does not wish a statement of his or her account or any mail sent to him or her.
- Customer asks many questions about how the financial institution disseminates information about the identification of its customers.
- A business customer is reluctant to provide complete information about the nature and purpose of its business, anticipated account activity and other details about the business or to provide financial statements or documents about a related business entity.
- Customer provides no record of past or present employment on a loan application.
- Customer's Internet Protocol (IP) address does not match the identifying information provided during online registration.

UNUSUAL CASH TRANSACTIONS

- Customer makes large cash deposit without having counted the cash or cannot justify source of funds or a comparison of proof of income does not justify amount being deposited or invested,
- Customer's cash contain counterfeit bills or musty or extremely dirty bills.
- Customer opens several accounts in one or more names, and then makes several cash investments under the reporting threshold.
- Customer requests payment to be made to offshore account
- Customer attempts to take back a portion of a cash that exceeds the reporting threshold after learning that a cash transaction report will be filed.
- Customer often deals in large amounts of cash and not negotiable instruments

UNUSUAL COMMERCIAL ACCOUNT ACTIVITY

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.
- Retail business that provides check-cashing services does not make withdrawals of cash against check deposits, possibly indicating that it has another source of cash.
- Customer maintains an inordinately large number of accounts for the type of business purportedly being conducted.
- Corporate account shows little or no regular, periodic activity.
- A transaction includes circumstances that would cause a banker to reject a loan application because of doubts about the collateral.

- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- Transacting businesses share the same address, provide only a registered agent's address or raise other address-related inconsistencies.

UNUSUAL INVESTMENT ACTIVITY

- Customer uses an investment account as a pass-through vehicle to wire funds to offshore locations.
- Investor seems uninterested in the usual decisions to be made about investment accounts, such as risks, commissions, fees or the suitability of the investment vehicles.
- Customer wants to liquidate a large position through a series of small transactions.
- Customer deposits cash, money orders, traveler's checks or cashier's checks in amounts under the reporting threshold to fund an investment account.
- Customer cashes out annuities during the free look period or surrenders the annuities early

UNUSUAL EMPLOYEE ACTIVITY

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires.
- Employee is involved in an excessive number of unresolved exceptions.
- Employee lives a lavish lifestyle that could not be supported by his or her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.
- Employee uses company resources to further private interests.
- Employee assists transactions where the identity of the ultimate beneficiary or counter party is undisclosed.
- Employee avoids taking periodic vacations.

UNUSUAL ACTIVITY IN A BROKER-DEALER SETTING

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information, or is otherwise evasive regarding that person or entity
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity

- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds from the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose
- The customer requests that a transaction be processed in such a manner so as to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, bearer bonds, which, are usually used in connection with fraudulent schemes and money laundering activity
- The customer's account shows an unexplained high level of activity with very low levels of securities transactions.

ANNEX B- TERRORIST FINANCING INDICATORS

UNUSUAL ACTIVITY INDICATIVE OF POTENTIAL TERRORIST FINANCING

The Egmont Group reviewed 22 terrorist financing cases submitted by financial intelligence units (FIUs) and compiled financial and behavioral indicators that were most frequently observed indicators associated to terrorist financing. Behavior indicators

- The parties to the transaction (owner, beneficiary, etc.) being from countries known to support terrorist activities and organizations
- Use of false corporations, including shell companies
- Inclusion of the individual in the United Nations 1267 Sanctions list
- Media reports that the account holder is linked to known terrorist organization or is engaged in terrorist activities
- Beneficial owner of the account is not properly identified
- Use of nominees, trusts, family member or third-party accounts
- Use of false identification
- Abuse of nonprofit organizations Indicators linked to financial transactions
- The use of funds by nonprofit organization is not consistent with the purpose for which it was established
- The transaction is not economically justified considering the account holder's business or profession
- A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds
- Transactions that are inconsistent with the account's normal activity
- Deposits were structured below the reporting requirements to avoid detection
- Multiple cash deposits and withdrawals with suspicious references
- Frequent domestic and international ATM activity
- No business rationale or economic justifications for the transactions
- Unusual cash activity in foreign bank accounts
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country
- Use of multiple foreign bank accounts

ANNEX C-RISK CATEGORIES

Country/ Geographic Risk

There is no universally agreed upon definition or methodology for determining whether a jurisdiction, in which the reporting entity operates, such as a particular country, geographic area or border region within a country, represents a higher risk for ML/TF.

Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF risks. Factors that may be considered as indicators of higher risk include:

a) Countries/areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
b) Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
c) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Organisation.
d) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions.

Customer/Investor Risk

Reporting Entities should determine whether a particular customer/investor poses higher risk and analyse the potential effect of any mitigating factors on that assessment. Such categorisation may be due to a customer's occupation, behaviour or activity.

These factors considered individually may not be an indication of higher risk in all cases. However, a combination of them may certainly warrant greater scrutiny. Categories of customers whose business or activities may indicate a higher risk include:

a) Customer is sanctioned by the relevant national competent authority for non-compliance with the applicable AML/CFT regime and is not engaging in remediation to improve its compliance.

b) Customer is a PEP or customer's family members or close associates are PEPs (including where a beneficial owner of a customer is a PEP) as covered under FATF Recommendation 12.

c) Customer resides in or whose primary source of income originates from high-risk jurisdictions (regardless of whether that income originates from a cash-intensive business).

d) Customer resides in countries considered to be uncooperative in providing beneficial ownership information.

e) Customer acts on behalf of a third party and is either unwilling or unable to provide consistent information and complete documentation thereon. f) Customer has been mentioned in negative

news reports from credible media, particularly those related to predicate offences for ML/TF or to financial crimes.

f) Customer's transactions indicate a potential connection with criminal involvement, typologies or red flags provided in reports produced by the FATF or national competent authorities (e.g. FIU, law enforcement etc.).

g) Customer is also a securities provider, acting as an intermediary or otherwise, but is either unregulated or regulated in a jurisdiction with weak AML/CFT oversight.

h) Customer is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business

i) The number of STRs and their potential concentration on particular client groups.

j) Customer is a legal entity predominantly incorporated in the form of bearer shares.

k) Customer is a legal entity whose ownership structure is unduly complex as determined by the securities provider or in accordance with any regulations or guidelines.

l) Customers who have sanction exposure (e.g. have business/activities/transactions).

m) Customer has a non-transparent ownership structure.

Product/Service/ Transactions Risk

A Reporting entity may offer a range of products/services to customers. An overall risk assessment should therefore include determining the potential risks presented by specific products and services offered by the reporting entity. These products and services commonly involve executing transactions for a customer by processing an order to transact or clear trades, handling the movement of funds or securities for the customer and settling a customer's transactions and liabilities.

The reporting entity may also offer brokerage accounts as a custodian of a customer's assets. Transactions may be conducted on a regulated exchange or other market or they may be conducted between parties directly. A reporting entity should assess, using a RBA, the extent to which the offering of its products and services presents potential vulnerabilities to placement, layering or integration of criminal proceeds into the financial system.

Determining the risks of products and services offered to a customer may include a consideration of their attributes, as well as any associated risk mitigation measures. Products and services that may indicate a higher risk include:

a) Products or services that may inherently favour anonymity or obscure information about underlying customer transactions (e.g. bearer share instruments or the provision of omnibus account services).

b) The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions.

c) Products with unusual complexity or structure and with no obvious economic purpose.

d) Products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction.

e) Use of new technologies or payment methods not used in the normal course of business by the securities provider.

f) Products that have been particularly subject to fraud and market abuse, such as low-priced securities.

g) The purchase of securities using physical cash.

h) Offering bank-like products, such as check cashing and automated cash withdrawal cards.

i) Securities-related products or services funded by payments from, or instructions given by unexpected third parties, particularly from higher risk jurisdictions.

j) Transactions involving penny/microcap stocks.

A customer may request transactions that pose an inherently higher risk to the reporting entity. This may be detected during transaction monitoring, although in many cases the customer's transactional activity may be apparent during both the point-of-sale interaction and back-end transaction monitoring.

Factors that may be considered as indicators of higher risk include:

a) A request is made to transfer funds to a higher risk jurisdiction/country/corridor without a reasonable business purpose provided.

b) A transaction is requested to be executed, where the securities provider is made aware that the transaction will be cleared/settled through an unregulated entity.

Distribution Channel Risk

An overall risk assessment should include the risks associated with the different types of delivery channels to facilitate the delivery of securities products and services. Securities products and services are typically distributed directly to customers (including online) or through intermediaries.

A reporting entity should analyse the specific risk factors, which arise from the use of intermediaries and their services. Intermediaries' involvement may vary with respect to the activity they undertake and their relationship with the securities providers. Some intermediaries may only introduce customers to the securities provider, whereas in other cases intermediaries may also use the products and services for their underlying customers (e.g. where the business relationship is established between intermediary and customer).

Regardless of the model, reporting entities should understand who the intermediary is and perform a risk assessment on the intermediary prior to establishing a business relationship. Reporting Entities and

intermediaries should establish clearly their respective responsibilities for compliance with applicable regulation.

Assessing intermediary risk is more complex for reporting entities with an international presence due to varying jurisdictional requirements, the potential risk of non-compliance by intermediaries with the applicable local AML/CFT regulations and the logistics of intermediary oversight. An intermediary risk analysis should include the following factors, to the extent that these are relevant to the securities providers' business model:

- Intermediaries suspected of criminal activities, particularly financial crimes or association with criminal associates.
- Intermediaries located in a higher risk country or in a country with a weak AML/CFT regime.
- Intermediaries serving high-risk customers without appropriate risk mitigating measures.
- Intermediaries with a history of non-compliance with laws or regulation or that have been the subject of relevant negative attention from credible media or law enforcement.
- Intermediaries that have failed to attend or complete AML/CFT training programmes requested by the securities providers.
- Intermediaries that have weak AML/CFT controls or operate substandard compliance programmes, i.e. programs that do not effectively manage compliance with internal policies and/or external regulation or the quality of whose compliance programmes cannot be confirmed.

Risk Mitigation in the Securities Sector

To enable the management and mitigation of identified risks reporting entities must:

(a) Have policies, controls and procedures, which are approved by senior management;

(b) Monitor the implementation of the controls and enhance them if necessary;

(c) Take enhanced measures where higher risks are identified; and

(d) Have appropriate mechanisms to provide risk assessment information to competent authorities and supervisory authorities.

APPROVED BY CHIEF EXECUTIVE OFFICER/GENERAL MANAGER:

Cheryl Ibbott

CHERYL IBBOTT

DATED THIS
30th January 2023

-END-