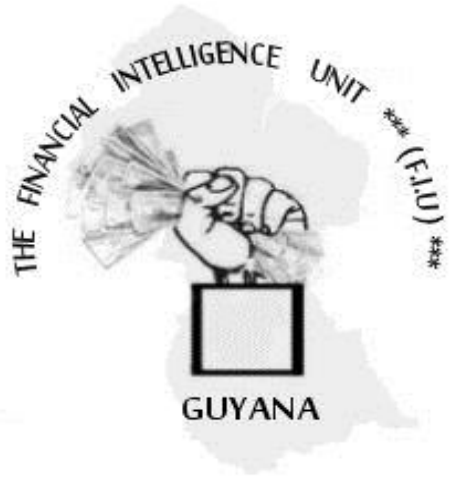


Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT)

Handbook

For

REPORTING ENTITIES

Published: February 18, 2021

Contents

FOREWORD

This Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Handbook aims to assist ***reporting entities*** in implementing measures to comply with their obligations under the AML/CFT legislation. It is designed to highlight the minimum requirements for a reporting entity's compliance with its AML/CFT legislative obligations. This Handbook should be used in conjunction with relevant guidelines published by the Financial Intelligence Unit (FIU), the AML/CFT Act and related local legislation, Guidance provided by AML/CFT Supervisory Authorities, as well as guidance and best practice papers published by the Financial Action Task Force (FATF).

INTRODUCTION

The FIU is of the sound view that the key to combatting money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction lies in the implementation of the country's comprehensive and consistent framework of measures and controls that are in place.

This Handbook aims at assisting reporting entities in meeting their obligations under the Anti-Money Laundering and Countering the Financing of Terrorism Act (AMLCFTA) No. 13 of 2009, the Anti-Money Laundering and Countering the Financing of Terrorism Regulations (AMLCFTR) No. 4 of 2010, and the AMLCFTR No. 4 of 2015 as amended, by providing guidance on matters thereof.

While this Handbook specifically targets the following Designated Non-Financial Business or Professions (DNFBPs) and the other types of reporting entities not classified as either DNFBPs or Financial Institutions (FIs), it may also be useful for FIs that also have the responsibility of implementing measures to combat the financing of terrorism in accordance with the requirements of the AML/CFT Act, Regulations and Guidelines and the FATF's Standards.

DNFBPs

- Casinos
- Lotteries
- Betting Shops
- Real Estate Agents, Brokers and Developers
- Dealers in Precious Metals (Gold Dealers)
- Dealers in Precious and Semi-Precious Stones (Licensed Traders)

- Attorneys-at-law, notaries, commissioner of oaths to affidavit, other legal professionals, accountants and auditors when they prepare for or carry out transactions for their client relating to the following activities:

    (i) Buying and selling real estate;
    (ii) Managing of client money, securities or other assets;
    (iii) Management of bank, savings or securities accounts;
    (iv) Organisation of contributions for the creation, operation or management of companies;
    (v) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

Other reporting entities

- Co-operatives including Credit Unions
- Registered Charities
- Pawnbrokers
- Used Car or Car Parts Dealers

LEGISLATIVE FRAMEWORK

Guyana has taken several important steps over the past years to enact legislative amendments to strengthen the country's AML/CFT regime. These legislative improvements include the enactment of the AMLCFT Amendment Act No. 15 of 2010, the AMLCFT Amendment Act No. 1 of 2015, the AMLCFT Amendment Act No. 10 of 2015, the AMLCFT Amendment Act No. 15 of 2016, the AMLCFT Amendment Act No. 21 of 2017, the AMLCFT Amendment Act No. 17 of 2018; the AMLCFT Regulation No. 4 of 2015, and the AMLCFT Amendment Regulation No. 7 of 2015.

MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

What is money laundering?

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, whereby avoiding prosecution, conviction and confiscation of the criminal funds.[1] It is commonly known as the "washing/laundering of dirty money". Simply put, money laundering is the process of making dirty money look clean.

[1] Combatting Money Laundering and Terrorist Financing – A Model of Best Practice for the Financial Sector the Professions and other Designated Businesses – Second Edition – Commonwealth Secretariat

The money laundering process

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.
- 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.

Examples of integration transactions include:

- Purchasing luxury assets like property, artwork, jewelry or automobiles
- Getting into financial arrangements or other ventures where investments can be made in business enterprises.

Money laundering is a criminal offence

According to Section 3(1) of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act 2009 as amended.

"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."

According to Sections 3(6) and (7) of the AML/CFT Act,

(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 nor more than one hundred million dollars*** and to ***imprisonment for seven years***, or

(ii) on conviction on indictment, to a fine of ***not less than ten million dollars nor more than one hundred and twenty million dollars*** and to ***imprisonment for ten 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 nor more than five hundred million dollars***; or

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

TERRORISM AND TERRORISM FINANCING

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.

Who is a terrorist?

The term terrorist refers to any natural person who:

(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 a terrorist organization?

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 terrorism financing?

Terrorism financing is the financing of terrorist acts, terrorists and/ or terrorist organisations.

Terrorist financing is a criminal offence

According to Section 68(1) of the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Act 2009 **as amended.**

"A person who by any means directly or indirectly, wilfully 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 organisation 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 together with death;***

(ii) in any other case, the punishment is a fine of ***not less than five hundred thousand dollars together with imprisonment for not less than ten years nor more than fifteen years***."

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 non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Proliferation financing is 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 nor more than one hundred millions dollars*** or to ***imprisonment for up to seven years*** and in the case of a body corporate to a fine of ***not less than ten million dollars nor more than two hundred million dollars***.

TARGETED FINANCIAL SANCTIONS[2] 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.

Prohibition/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.

[2] Targeted Financial Sanctions means both assets 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

(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.[3]

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

THE FINANCIAL INTELLIGENCE UNIT

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 unit is established and operates under section 9 (1) of the AML/CFT Act 2009 as amended.

Core and other functions of the FIU

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

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.

[3] Sections 68A(2) and 68E(2) of the AML/CFT Act 2009 as amended

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 its intelligence.

SUPERVISORY AUTHORITIES

Supervisory authorities are designated competent authorities with responsibilities aimed at ensuring compliance by reporting entities with the requirements of the AML/CFT legislation to combat money laundering and terrorist financing.

Below is a list of supervisory authorities and their respective reporting entities:

Supervisory Authority	**Reporting Entities**
Governor, Bank of Guyana	• Commercial Banks • Money Transfer Agencies • Cambios • Insurance Companies and Brokers • Non-Bank Financial Institutions
Guyana Securities Council	• Securities Companies and Brokers
Guyana Gold Board	• Dealers in Precious Metals (Gold Dealers)
Guyana Geology & Mines Commission	• Dealers in Precious and Semi-Precious Stones (Licensed Traders)
Guyana Revenue Authority	• Pawnbrokers • Used Car Dealers • Real Estate Agents
Gaming Authority	• Casinos • Lotteries • Betting Shops
Departments of Cooperative & Friendly Societies	• Cooperatives including Credit Unions • Registered Charities

Key obligations of a supervisory authority

To ensure that reporting entities are compliant with their obligations under the AML/CFT legislation, supervisory authorities have powers and responsibilities to:

- Examine and supervise the reporting entities, and regulate and oversee effective compliance with the obligations set out in the AML/CFT legislation and any other preventive measures in relation to combating money laundering and terrorist financing;

- Issue instructions, guidelines or recommendations and provide training to reporting entities on their obligations and requirements under the AML/CFT legislation;

- Ensure that their reporting entities update their AML/CFT Compliance Program in keeping with any amendments to the AML/CFT legislation.

- Enter into the business premises of a reporting entity during ordinary working hours in order to: (i) inspect or take documents or make copies or extracts of information from such documents; (ii) inspect premises; and (iii) observe the manner in which certain functions are undertaken, and require any person on the premises to provide an explanation on any such information.

- Impose sanctions on reporting entities for non-compliance with AML/CFT obligations; and the FIU accordingly.

SANCTIONS FOR NON-COMPLIANCE WITH AML/CFT OBLIGATIONS

Administrative Sanctions

Supervisory authority can impose administration sanctions on a reporting entity that fails to comply with its obligations under the AML/CFT legislation. These sanctions include:

- Written warnings
- Order to comply with specific instructions
- Order regular reports from the RE on the measures it is taking
- Prohibit a convicted person from employment within the RE
- Recommend to appropriate licensing authority of the reporting entity (where the supervisory authority is not such) that the reporting entity's licence/registration be suspend, restrict or withdraw.
- Removal of defaulting director or senior manager from board.
- A fine of ***five to fifteen million dollars***.

Criminal sanctions

A reporting entity or any of its directors, managers, officers or employees that breaches its obligations under the AML/CFT legislation can also be sanctioned criminally.

In the case of a breach by an individual, the penalty is a fine of ***five to fifteen million dollars***; and ***imprisonment for up to three years***, and in the case of a breach by a company/body corporate, the penalty is a fine of between ***fifteen to forty million dollars***.

REPORTING ENTITIES

Who is a reporting entity?

A Reporting Entity is any person or entity carrying out any activity listed in the First Schedule of the AML/CFT Act 2009. Entities that have been classified as reporting entities by virtue of the activities they engage in are as follows:

Licensed Financial Institutions	**Designated Non-Financial Businesses of Professions**	**Other**
• Commercial Banks • Non-Bank Financial Institutions • Money Transfer Agency • Cambios • Insurance Companies and Brokers • Securities Companies and Brokers	• Casinos • Lotteries • Betting Shops • Real Estate Agents, Brokers and Developers • Dealers in Precious Metals (Gold Dealers) • Dealers in Precious and Semi-Precious Stones (Licensed Traders) • Attorneys-at-Law, Notaries, and Commissioner of Oaths to Affidavit • Accountants and Auditors • Trusts or Company Service Providers	• Co-operatives including Credit Unions • Registered Charities • Pawnbrokers • Used Car or Car Parts Dealers

REQUIREMENTS OF REPORTING ENTITY

Reporting entities must: -

(a) 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;

(b) Establish and maintain internal policies, procedures, controls and systems for customer identification, record keeping and retention, monitoring, reporting, making employees aware of AML/CFT laws, making employees aware of entity's policies and procedures to deter ML/TF, and screening persons before hiring them;

(c) Establish and maintain independent audit function to test its AML/CFT procedures and systems;

(d) Train its employees on an on-going basis to recognize suspicious transactions and to be kept informed of new developments, including information on current ML/TF techniques, methods and trends as well as their obligations under the AML/CFT legislation relating to Customer Due Diligence (CDD) and Suspicious Transaction Report (STR);

(e) Identify and assess ML/TF risks related to new technologies;

(f) Register with the FIU in such manner and form as determined by the Director;

(g) Apply appropriate countermeasures to higher-risk countries; and

(h) Assess risks and apply a risk-based approach.

Compliance Officer

Guidance for appointing compliance officer

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.

Internal policies, procedures, controls and systems

The reporting entity's policies, procedures, and controls should be designed to prevent, detect, and deter money laundering and terrorist financing. These should be included in the entity's AML/CFT Compliance Programme which must be established in writing and signed off by senior management before submitting to the FIU for approval.

Guidance for establishing internal policies, procedures, controls and systems

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;

(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.

Audit function

The reporting entity's AML/CFT program must be monitored and evaluated. It must be assessed regularly to ensure their effectiveness and to look for new risk factors.

The audit must be independent, meaning that it must not be performed by persons involved with the entity's AML/CFT compliance staff. Individuals conducting the audit should report directly to the board of directors or senior management (whichever is applicable).

Guidance for establishing and maintaining independent audit function

The independent audit should at a minimum:

- Assess the overall integrity and effectiveness of the AML/CFT compliance program, including policies, procedures and processes.
- Assess the adequacy of the AML/CFT risk assessment.
- Examine the adequacy of CDD policies, procedures and processes, and whether they comply with regulatory requirements.
- Determine personnel adherence to the entity's AML/CFT policies, procedures and processes.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations).
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.
- Assess compliance with the AML/CFT Act, Regulations and Guidelines.
- Examine the integrity and accuracy of management information systems used in the AML/CFT compliance program.
- 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.
- Assess the effectiveness of the entity's policy for reviewing accounts/transactions that generate multiple suspicious transaction report filings, including account closure processes.
- Assess the adequacy of record-keeping and record retention processes.

- Track previously identified deficiencies and ensure management corrects them promptly.
- Consider whether the management of the entity was responsive to earlier audit findings.
- 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.

AML/CFT training

Training is one of the most important ways to ensure that AML/CFT measures as specified in AML/CFT legislation and relevant guidelines are being implemented by the reporting entity. While there is no single or definitive way to conduct training, the critical requirement is that training is adequate and relevant to those being trained and that the content of the training reflects good practice.

Guidance for AML/CFT training

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.
- 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.

A. Identifying and assessing ML/TF risks related to new technologies

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.

Guidance for new technologies

- 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.

Registering with the Financial Intelligence Unit (FIU)[4]

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.

Guidance for registering with the FIU
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

[4] Section 19(4) of the AML/CFT Act 2009 as amended

Apply appropriate countermeasures to higher-risk countries

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) of higher risk countries - countries with strategic AML/CFT deficiencies that FATF identifies as (i) High-Risk Jurisdictions subject to a Call for Action, and (ii) Jurisdictions under Increased Monitoring.

Assessing risks and applying a risk-based approach

Risk assessment

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.

Risk mitigation

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.

CUSTOMER DUE DILIGENCE[5]

Legislative requirement:

Reporting entities to identify and verify identity of customer – s. 15 AML/CFT 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.

[5] Section 15 of the AML/CFT Act 2009 as amended

Standard 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*[6] 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 conducted are consistent with the business and risk profile of the customer, including, where necessary, the *source of wealth*[7] and *source of funds*[8].

Guidance for implementing Standard CDD measures:

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*:

[6] 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 arrangement.

[7] Source of wealth focuses on where the customer's wealth originated. Acceptable sources that validate source of wealth include: Proof of property sale, records of investment, commercial loan agreement letter, audited financial statements, written confirmation from a qualified accountant/lawyer, or grant of probate/copy of will.

[8] Source of funds focuses on where the funds used for the transaction originated from – location/entity/format. Funds may originate from the sale of asset, salary, or earnings from business ownership or business activities.

- 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.

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 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)
- 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.

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 ID of the person appearing on behalf of the government organization/ministry/statutory body

*To verify the identity of a customer that is a government o*rganization, 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 (company/partnership etc.) -

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

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 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[9] wishes to establish a business relationship[10] 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;

(d) There are doubts about the accuracy or adequacy of previously obtained customer identification data;

(e) Completing a transaction for an occasional customer[11]; or

[9] Customers include persons, whether natural, legal or legal arrangement.

[10] A business relationship is 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.

[11] An '**occasional transaction**' is a cash **transaction** that occurs outside of a business relationship (the **transaction** may be carried out in a single operation or several operations that appear to be linked).

(f) Completing a transaction for a high-risk customer, for example, non-resident customer, politically exposed person etc.

Note:
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 is prohibited from carrying 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 is to consider submitting a Suspicious Transaction Report (STR) to the FIU.

Enhanced CDD

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.

Guidance for applying enhanced CDD measures:

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.

The reporting entity must also conduct enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

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

Political Exposed Persons

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 organisation PEP or Foreign PEP respectively).

To identify and verify the identity of a customer that is a PEP:

- The reporting entity must adequately identify and verify the customer's identity by obtaining the information required to identify and verify the identity of a natural person (see above).

In addition, the reporting entity must:

- Have appropriate risk management systems to determine whether the customer is a PEP; and
- implement enhanced CDD measures.

Non-Face-to-Face Customer[12]

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.

[12] Customers that are not physically present for the purposes of identification and verification (potentially high-risk customer)

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 customers[13]

The reporting entity must pay attention to non-resident/foreign customers (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[14]

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;

[13] Foreign customers are natural or legal persons existing under the laws of a foreign country and their principal address or place of business is located in a foreign country other than Guyana - (potentially high-risk customer)

[14] A third party/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.

(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.

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

RECORD KEEPING[15]

Legislative requirement:

Reporting entities to maintain all records of its customer's transaction for at least seven years from the date the relevant transaction was completed, or termination of business relationship, whichever is later. s. 16 AML/CFT Act 2009 as amended.

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 keeping records

What records must be kept?

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

- Records of the evidence of the customer's identity (e.g. copies or records of official identification documents like passports, ID cards, driving licences);

[15] Section 16 of the AML/CFT Act 2009

- Records of account files and business correspondence in relation to transactions and identities of persons involved in the transactions (e.g. inquires 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 nature and date of the transaction;

- 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.

How are records to be maintained?
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*[16]; 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.

[16] Questions from a competent authority pertaining to a customer and transactions conducted by that customer.

REPORTING

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

- Threshold Transaction Reports,
- Suspicious Transaction Reports, and
- Terrorist Property Reports.

Threshold transaction reports (TTRs)

TTRs are reports of transactions conducted by customers of reporting entities that meet pre-determined limits/ thresholds. For example, any cash (or non-cash in some specific instances) transaction facilitated by a reporting entity for a customer (single or accumulated) within a month that meets the following threshold limit:

Reporting Entity	**Reporting Threshold**
• Commercial Banks, • Insurance Companies and Brokers • Securities Companies and Brokers • Used Car or Car Parts Dealers, • Real Estate Agents, Brokers and Developers • Dealers in Precious Metals (Gold Dealers) • Dealers in Precious and Semi-Precious Stones (Diamond Dealers)	any cash transaction equal to or above **G$2,000,000**
• Casinos • Betting Shops* • Lotteries • Credit Unions	any cash transaction equal to or above **$500,000** *A special threshold of **$60,000** has been set for some betting shops.
Cambio	any foreign currency purchase above **G$400,000**, and sale over **G$1,000,000**
Pawnbrokers	any cash transaction above **$300,000**
Money Transfer Agencies	any money transfer (sent or received) above **G$200,000**

TTRs are due by the 7th of each month following the month in which the transaction(s) occurred and should be reported in such manner or format prescribed by the Director of the FIU.

Important Note:

The following categories of reporting entities have been exempted by the FIU from the submission of threshold transactions:

- Attorneys-at-Law, Notaries, and Commissioner of Oaths to Affidavit
- Accountants and Auditors
- Trusts or Company Service Providers

- Registered Charities
- Cooperative Societies

Suspicious transaction report (STR)

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

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

Guidance for suspicious transaction reporting

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).

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.

The FIU relies on reporting entities to fulfill their obligation to report suspicious transactions/activities. STRs are the main source of information available to the FIU to detect suspected money laundering or predicate/serious offences. An STR can indicate that suspected criminal activity is occurring through a transaction or series of transactions. Reports received by the FIU are analyzed for activities and patterns that may indicate criminal activity. Various resources are used including partner agencies and open-source databases. Often, additional information is required from reporting entities to help establish whether the suspicious activity reported in an STR merits further investigation. This additional information can be vital in determining whether the suspicion translates into actual criminal activity. Where criminal activity appears to be occurring, cases may be referred to the Special Organised Crime Unit or other relevant law enforcement agency for investigation.

Terrorist property report (TPR)

A TPR is a report that a reporting entities 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 has been identified as having the beforementioned association.

Guidance for terrorist property reporting

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)

[17] Regulation 5(3) of AML/CFT Regulations No. 4 of 2015 as amended

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.

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 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 on: https://fiu.gov.gy

Conducting 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.

Where to send reports

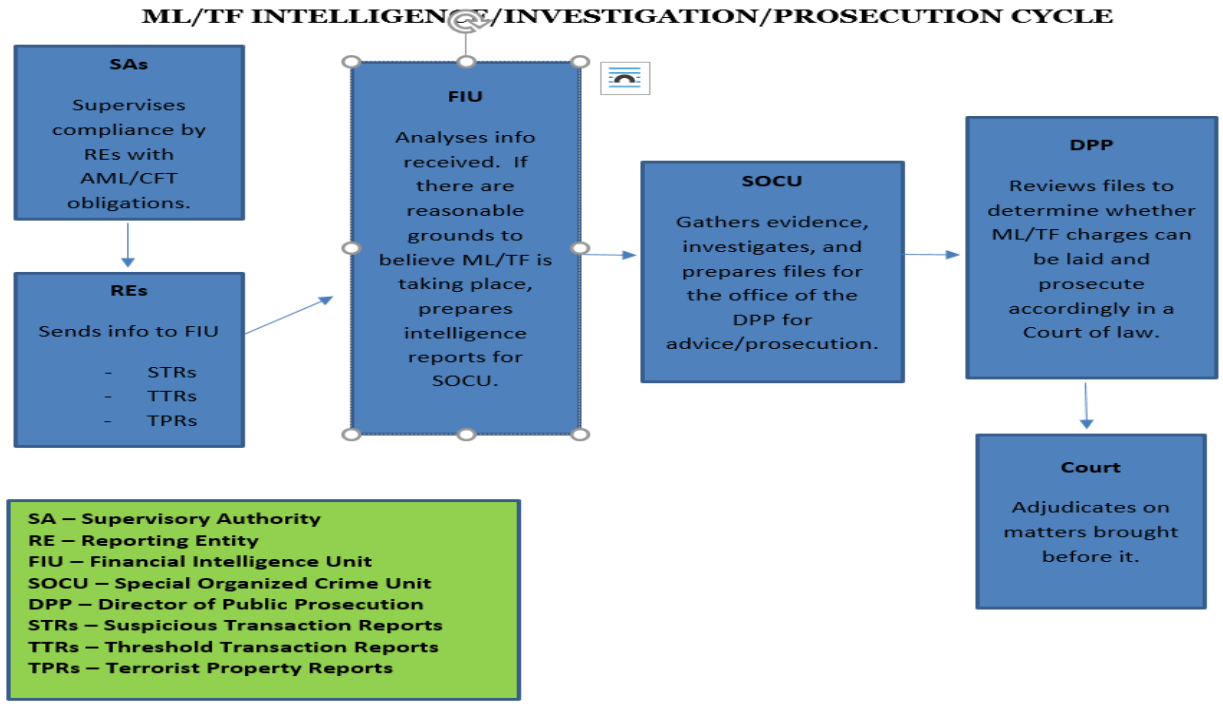
Reports can be submitted to the FIU electronically (via the FIU's secured e-reporting platform - CaseKonnect) or on CD/USB hand delivered. To submit report electronically a reporting entity must first be registered on the FIU Electronic Reporting Platform. To register the reporting entity must send a letter to the FIU requesting authorization. The letter must state the full name, designation, telephone number, and email address of the person to be authorized (e.g. the reporting entity's compliance officer) and the name and address of the reporting entity.

Paper/CD reports must be submitted to:

Director
Financial Intelligence Unit
c/o Ministry of Finance
Main and Urquhart Streets
Georgetown

Note:
All Forms (TTR/STR/TPR) for reporting other than through the secured medium, can be accessed from the FIU's website fiu.gov.gy.

What becomes of your reports when submitted to the FIU?



TIPPING-OFF

A reporting entity, its directors, officers or employees are prohibited from disclosing (tipping-off) the fact that a suspicious transaction report or related information is being filed with the FIU[18].

It is an offence for a person who knows or suspects that a report is being prepared or has been sent to the FIU, to disclose that information to another person, other than a court, or other person authorized by law.

A person who commits this offence shall be liable to 'a fine of not less than one million dollars (G$1,000,000.00) and to imprisonment for three (3) years.

NO CRIMINAL OR CIVIL LIABILITY FOR INFORMATION

A reporting entity, its directors, officers or employees are protected from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.[19]

[18] Section 5 of the AML/CFT Act 2009 as amended

[19] Section 11 of the AML/CFT Act 2009 as amended

ANNEX: MONEY LAUNDERING INDICATORS/RED FLAGS

While there is no exhaustive list of tried-and-true suspicious activity indicators for reporting entities, below are some common indicators or "red flags" that may indicate a link to financial crime or money laundering activities:

Money Laundering

1. Customer admits or makes statements about involvement in criminal activities.
2. Customer does not want correspondence sent to home address.
3. Customer appears to be active with several similar institutions in one area for no apparent reason.
4. Customer conducts transactions at different physical locations within a short period, in an apparent attempt to avoid detection.
5. Customer has travelled from a far location to conduct business with your entity when there are similar entities closer to where they reside/work.
6. Customer repeatedly uses an address but frequently changes the names involved.
7. Customer is accompanied and watched.
8. Customer shows uncommon curiosity about internal systems, controls and policies.
9. Customer has only vague or confusing knowledge of the amount and other details of the transaction.
10. Customer over justifies or explains the transaction.
11. Customer is secretive and reluctant to meet in person.
12. Customer is nervous for no obvious reason, while completing the transaction.
13. Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact the customer using information they provided.
14. Normal attempts to verify the background of a new or prospective customer are difficult.
15. Customer appears to be acting on behalf of a third party but does not voluntarily disclose same.
16. Customer is involved in activity that in not in keeping with the profile of that individual or business.
17. Customer insists that the transaction be done quickly.

18. Inconsistencies appear in the customer's presentation of the transaction.

19. The transaction does not appear to make business or economic sense.

20. Customer attempts to develop close rapport with staff (maybe to distract or adversely affect their focus).

21. Customer uses aliases and a variety of similar but different addresses.

22. Customer spells his or her name differently from one transaction to another.

23. Customer provides false information or information that you believe is unreliable.

24. Customer offers you money, gratuities or unusual favours for the provision of services, which appears unusual or suspicious.

25. Customer pays for services or products using unusual methods such as precious minerals, 3rd party financial instruments such as money orders or traveller's cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes, etc.

26. You are aware that a customer is the subject of a money laundering or terrorist financing investigation.

27. You are aware, or you become aware, from a reliable source (that can include media or other open sources), that a customer is suspected of being involved in illegal activity.

28. Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

Knowledge of reporting or record keeping requirements

1. Customer attempts to convince an employee not to complete documentation that is required for the transaction.

2. Customer makes inquiries that would indicate a desire to avoid reporting.

3. Customer has unusual knowledge of the law in relation to suspicious transaction reporting.

4. Customer seems very conversant with money laundering or terrorist activity financing issues.

5. Customer is quick to volunteer that funds are “clean” or “not being laundered.”

6. Customer performs two or more cash transactions of less than the threshold limit each within a short period, seemingly to avoid the accumulated rule.

Identity documents

1. Customer provides doubtful or vague information.
2. Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
3. Customer refuses to produce personal identification documents.
4. Customer wants to establish identity using something other than his or her personal identification documents.
5. All identification presented is foreign or cannot be checked for some reason.
6. All identification documents presented appear new or have recent issue dates.
7. Customer alters the transaction after being asked for identity documents.
8. Customer presents different identification documents each time a transaction is conducted.

Cash transactions

1. Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past.
2. Customer frequently exchanges small bills for large ones.
3. Customer uses notes in denominations that are unusual for the customer, when the norm in that business is different.
4. Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.
5. Customer transacts business with smelly or extremely dirty/soiled bills.
6. Customer makes cash transactions of consistently rounded-off large amounts
7. Customer presents uncounted funds for a transaction. Upon counting, the customer reduces the transaction to an amount just below that which could trigger reporting requirements.
8. Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
9. Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (i.e., student, unemployed, self-employed, etc.)

10. Cash is transported by a cash courier.

11. Large value transactions are conducted using a variety of denominations.

Economic purpose

1. Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the customer.

2. Transaction is unnecessarily complex for its stated purpose.

3. Activity is inconsistent with what would be expected from the declared business.

4. A business customer refuses to provide information to qualify for a business transaction.

5. No business explanation for size of transactions or cash volumes.

6. Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

Transactions involving areas outside of Guyana

1. Customer and other parties to the transaction have no apparent social or economic ties to Guyana.

2. Transaction crosses many international lines.

3. Use of a credit card issued by a foreign bank that does not operate in Guyana by a customer that does not live and work in the country of issue.

4. Transaction involves a country known for highly secretive banking and corporate law.

5. Transactions involving any country deemed by the Financial Action Task Force as requiring enhanced surveillance.

6. Foreign currency exchanges that are associated to locations of concern, such as countries known or suspected to facilitate money laundering activities.

7. Transaction involves a foreigner from a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.

8. Transaction involves a country known or suspected to facilitate money laundering activities.