ANTI-MONEY LAUNDERING/ COMBATING TERRORIST FINANCING & PROLIFERATION GUIDELINE FOR ATTORNEYS-AT-LAW

NO 1 OF 2023

Issued by the Antimoney Laundering/Countering the Financing of Terrorism/Proliferation Financing National Coordination Committee

July 2023

(UPDATED AUGUST 2023)

TABLE OF CONTENTS

ACRONYMS

AML/CFT Anti-money laundering and countering the financing of terrorism
CDD Customer Due Diligence
DNFBP Designated Non-Financial Business or Profession
FATF Financial Action Task Force
FIU Financial Intelligence Unit
GCC Guyana Compliance Commission
KYC Know Your Customer
NRA National Risk Assessment
PEP Politically Exposed Person
RBA Risk Based Approach

INTRODUCTION

The global threats of money laundering, and the financing of terrorism and proliferation of weapons of mass destruction have led the National Coordinating Committee (NCC) to strengthen Guyana's AML/CFT/PF regime in support of the efforts of Government of Guyana to combat money laundering, terrorist financing and proliferation financing.

Under the section 18 (11), as well as the **First Schedule of the Anti- Money Laundering and Countering the Financing of Terrorism Act 2009 (as amended),** designated Non-Financial Business or Profession' (DNFBP) includes, inter alia, **attorneys-at-law**, notaries, **other independent legal professionals** and accountants when they prepare for or carry out transactions for their client relating to the following activities—

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

Attorneys-at-Law, as a designated non-financial business or profession, are reporting entities pursuant to the Fourth Schedule of the AML/CFT Act 2009 as amended**.**

It is necessary for DNFBPs, which include attorneys-at-law, to be regulated to keep them safe from nefarious activities, and to protect the legitimate financial system from illegitimately acquired funds that could find their way into the financial system via these non-financial entities.

PURPOSE OF GUIDELINE

The Purpose of this Guideline is to provide guidance to all Attorneys-at-Law on their obligations under the AML/CFT Act 2009 as amended, and in doing so, comply with the Anti-Money Laundering and Financing of Terrorism and Proliferation requirements of the FATF Recommendations.

This Guideline, which is being issued pursuant to **Section 7A (6) (e) of the AML/CFT Act 2009 (as amended).**

APPLICATION

This Guideline applies to all persons and entities operating as attorneys-at-law, whether as business owners or sole practitioners, when they are performing the functions set out in the First Schedule of the AML/CFT Act 2009 as amended.

This Guideline is expected to be followed by principals and their agents. For the purpose of this Guideline, an attorney-at-law means a person registered as an attorney-at-law in Guyana. However, it does not refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering/terrorism financing/proliferation financing.

Some attorneys-at-law may be able to conclude that based on the services they provide, they do not have any specific AML/CFT obligations as they do not prepare for, or carry out any of the functions set out above. However even though specific AML/CFT obligations may not apply to an attorney-at-law, it is consistent with the overall ethics and best practices of the profession for all attorney-at-laws to ensure that their services are not being misused, including by criminals. Accordingly, attorney-at-laws should carefully consider what they need to do to guard against that risk, in order not to be unwittingly involved in ML/TF.

This Guideline shall be considered in the context of applicable professional privilege and professional secrecy rules. Privilege/professional secrecy is a protection to the client, and a duty of attorney-at-law to protect client information or advice from being disclosed. In situations where attorney-at-laws are claiming professional privilege or professional secrecy, they must be satisfied that the information is protected by the privilege/professional secrecy and the relevant rules.

Designated Non- Financial Business or Profession (DNFBPs) are also to be guided by ***Financial Intelligence Unit- Guideline No. 2 of 2021 (updated June 2021) on DNFBPs AML/CFT Compliance Regime.*** ***https://fiu.gov.gy/wp-content/uploads/2022/12/DNFBP-AMLCFT-Compliance-Regime-Guideline-No-2-of-2021-PDF.pdf***

MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

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. It is commonly known as the "washing/laundering of dirty money". Simply put, money laundering is the process of making dirty money look clean.

The Money Laundering Process often involves:

(i) The **placement** of the proceeds of crime into the financial system, sometimes by techniques such as structuring currency deposits in amounts to evade reporting requirements or co-mingling currency deposits of legal and illegal enterprises;

(ii) The **layering** of these proceeds by moving them around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail; and

(iii) **Integrating** the funds into the financial and business system so that they appear as legitimate funds or assets.

FINANCING OF TERRORISM

Terrorism is the act of seeking for political, religious or ideological reasons to intimidate or compel others to act in a specified manner. A successful terrorist group, much like a criminal organization, is generally able to obtain sources of funding and develop means of obscuring the links between those sources and the uses of the funds. While the sums needed are not always large and the associated transactions are not necessarily complex, terrorists need to ensure that funds are available to purchase the goods or services needed to commit terrorist acts. In some cases, persons accused of terrorism may commit crimes to finance their activities and hence transactions related to terrorist financing may resemble money laundering.

It is worth emphasizing that while money laundering is concerned with funds generated from unlawful sources, funds used for terrorist activities are often legitimate in nature. The source of funds is, therefore, not the sole consideration for agents. The conversion of assets into money and the subsequent direction of that money must be observed.

As information changes, the United Nations publish lists of terrorist or terrorist organizations. Financial institutions and designated non-financial businesses and professionals are required to remain abreast of this information and check their databases against these lists. Should any person or entity on the lists be clients, that information should be immediately communicated to the FIU and the Special Organized Crime Unit.

The FATF Recommendations place obligations on countries as they relate to terrorist financing in the context of national cooperation and coordination, confiscation and provisional measures and targeted financial sanctions related to terrorism and terrorist financing. The latter is applicable to all United Nations Security Council resolutions (UNSCRs) applying targeted financial sanctions relating to the financing of terrorism. The Supervisory Authority's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting terrorism.

FINANCING OF PROLIFERATION

The FATF defines proliferation financing as "*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*.[1]".

Proliferation of weapons of mass destruction can take many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles). The Supervisory Authority's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting such proliferation.

[1] http://www.fatfgafi.org/topics/methodsandtrends/documents/typologiesreportonproliferationfinancing.html

INTERNATIONAL INITIATIVES

The FATF Forty Recommendations were revised in February 2012, and renamed the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations. The Recommendations were since updated in

- February 2013 (Mutual Legal Assistance and other forms of International Cooperation);
- October 2015 (Interpretative Note on Foreign Terrorist Fighters);
- June 2016 (Note on Non-profit Organizations);
- October 2016 (Interpretative Note on Terrorist Financing Offence);
- June 2017 (Interpretive Note on Targeted Financial Sanctions related to proliferation);
- November 2017 (on Tipping-off and Confidentiality and Interpretive Note on internal controls and foreign branches and subsidiaries);
- February 2018 (on National Cooperation and Coordination); and
- October 2018 (on New Technologies).

The FATF normally issues Guidance and Best Practices Papers to assist countries in implementing the Recommendations. Attorney-at-law should keep abreast of developments in the international standard and refine their programmes accordingly.

LEGISLATIVE AND REGULATORY FRAMEWORK

The Government of Guyana has enacted several pieces of legislation aimed at preventing and detecting drug trafficking, gold smuggling, corruption, money laundering, terrorist financing and other serious crimes. The Acts which are most relevant for the purposes of this Guideline are as follows:

1. The Anti Money Laundering and Countering the Financing of Terrorism Act 2009
    - 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 (Amendment) Act 2023
    - AMLCFT Regulation No. 4 of 2010
    - AMLCFT Regulation No. 4 of 2015
    - AMLCFT Regulation No. 7 of 2015
2. Anti-Terrorism and Terrorist Related Activities Act No. 15 of 2015
3. Narcotic Drugs and Psychotropic Substances (Control) Act
4. Mutual Assistance in Criminal Matters Act No. 38 of 2009
5. Criminal Law (Offences) Act No. 18 of 1893 as amended

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

The core functions of the FIU are outlined under ***Section 9(4) of the AMLCFT Act*** 2009 as amended. 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 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 or PF 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 intelligence with regard to money laundering, proliferation financing, 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.

Where an attorney-at-law is uncertain about how to treat an unusual or suspicious transaction, the attorney-at-law is strongly urged to speak directly to the FIU for preliminary guidance and then make a report as appropriate.

Suspicious Transaction Forms and Terrorist Property Reporting Forms may be accessed on the FIU's website: https://fiu.gov.gy/essential-forms/

GATEKEEPERS

Gatekeepers are businesses or professionals that are able to provide access into the financial system, including Attorneys-at-Law. They have the ability to allow illicit funds into the financial system, whether knowingly or not. This informs why it is necessary to regulate their activities for anti-money laundering purposes, although they are not financial institutions.

THE ROLE OF THE ATTORNEY-AT-LAW

Attorneys-at-law serve as gatekeepers since they have the ability to furnish access (knowingly or unknowingly) to the financial system through the various functions they perform that might help the criminal with funds to move or conceal them.

Professional expertise that attorneys-at-law provide may be important to a money laundering enterprise. For example, legal expertise is needed to set up complex corporate structures, or facilitate a sale of land transaction, which may not be easily detectable, especially where organized crime is involved.

Attorneys-at-law must see anti-money laundering policies and procedures as part of their operational practice. The consequences of participation in money laundering activity, or failing to prevent one's practice from being used in furtherance of this activity, are severe. Practitioners should refer to the penalty provisions of **the AML/CFT Act 2009.**

The AML/CFT Act expressly provides that its provisions apply to DNFBPs in the same way as it applies to financial institutions. This means that the duties contained in the legislation for financial institutions, also form part of the responsibilities of attorneys-at-law and other DNFBPs. This requires attorneys-at-law to keep client records and carry out due diligence procedures in seeking to properly know their clients. They are also duty bound to submit suspicious transaction reports to the FIU when the need arises. In order to make a proper judgment in this regard, they will need to avail themselves of training opportunities so that they may be properly equipped to protect themselves and their practices.

The issue of attorney-client privilege looms large over the responsibility of attorneys to report their clients' suspicious activity to the authorities. This Guideline does not intend to compromise this important principle of the legal profession. However, the law is blind when it comes to determining the profession of a person engaged in a money laundering enterprise, or a regulated professional who fails to report such activity.

It is important to assert here that the AML/CFT/PF National Coordination Committee understands that as part of the right to an effective legal defence, a client must be free to disclose the circumstances of his/her case fully to his/her legal representative, without fear of counsel passing that information, shared in confidence, to any authority. One does not anticipate that this will include counselling in money laundering, terrorism financing or proliferation financing.

It is worth emphasizing that the anti-money laundering responsibilities of an attorney-at-law arise only in the circumstances set out in the legislation and not to the general practice of all aspects of legal practice.

Even though individual attorneys-at-law or law firms may be able to conclude that specific AML/CFT obligations do not apply to them, ethical standards require them to ensure that their

services are not being misused, including by criminals, and they should carefully consider what they need to do to guard against that risk.

RISK BASED APPROACH (RBA)

The RBA to AML/CFT means that countries, competent authorities and DNFBPs including Attorneys-at-Law, should identify, assess and understand the ML/TF risks to which they are exposed and take the required AML/CFT measures effectively and efficiently, to mitigate and manage the risks.

According to the FATF Recommendations, reporting entities must are required to establish and maintain appropriate and risk-sensitive policies and procedures approved by its supervisory body-

(a) the performance and documentation of any products or services (prior to launch) and the continual documentation of risk assessment and management of such products and services, are provided in a form which is available to share with competent authorities and supervisory authorities and

(b)risk mitigation mechanisms which include : (i) consideration of the national risk assessment or of the reporting entity's risk assessment results or conclusions; (ii) the ability to effectively supply information to the supervisory authority; and (iii) the application of enhanced measures where the reporting entity's risk assessment identify a higher risk

(c) the monitoring and management of compliance with and the internal communication of such policies and procedures in order to prevent activities related to money laundering and terrorist financing.

The FATF Recommendations also indicate that reporting entities are required to take appropriate steps (including the use of risk mitigation mechanisms to –

(a) Identify, assess and understand its money laundering and terrorist financing risks depending on the type of customers business relationships, countries or geographic areas, services, delivery channels, products or transactions
(b) document the risk assessments and keep them updated

KEY ELEMENTS OF A RISK BASED APPROACH CAN BE SUMMARIZED AS FOLLOWS:

(i) **Risk Identification and Assessment -** identifying ML/TF risks facing a firm, given its customers, services, countries of operation, also having regard to publicly available information regarding ML/TF risks and typologies

(ii) **Risk Management and Mitigation** - identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks

(iii) **Ongoing Monitoring** - putting in place policies, procedures and information systems to monitor changes to ML/TF risks

(iv) **Documentation** - documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks

The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive measures and controls conducted should be stronger in higher risk scenarios.

However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

Implementing a RBA requires that attorneys-at-law have a sound understanding of the ML/TF risks and are able to exercise good professional judgement. Above all, attorneys-at-law and the leadership of law firms should recognise the importance of a culture of compliance across the organization and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of the organization. This requires the 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on ML/TF risks, both at the country and institutional levels, and to develop procedures and systems.

In this regard, attorneys-at-law are encouraged to pay close attention to their practice and apply defensive measures that are in proportion to the risk faced at any particular time. In the interest of clarity, attorneys-at-law should deploy defensive resources only where there is a threat of money laundering or financing of terrorism and proliferation. Further, the extent of that deployment should be a function of the extent of the risk faced.

As general guidance, the following considerations should be at the base of all due diligence actions:

(i) The nature and scale of the business;

(ii) The complexity, volume and size of transactions;

(iii) Type of client (e.g. whether ownership is highly complex, whether the client is a PEP, whether the client's employment income supports business activity, whether client is known to the justice system);

(iv) Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash transactions);

(v) Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking or corruption, whether the client is subject to regulatory or public disclosure requirements); and

(vi) Value of business and frequency of transactions.

Attorneys-at-law are required to regularly review their AML/CFT systems and test them for effectiveness. Records should be reviewed to ensure that all existing customer records are current and valid. Wherever beneficial ownership information is required, it must be borne in mind that the true beneficial owner is the ultimate beneficial owner. The ultimate beneficial owner (UBO) is the natural person who controls or benefits from the assets of the business.

For attorneys-at-law identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions where they operate, and the effectiveness of their controls in place, will require the investment of resources and training.

RISK IDENTIFICATION AND ASSESSMENT

Potential ML/TF risks faced by attorneys-at-law will vary according to many factors including the activities undertaken by them, the type and identity of the client, and the nature and origin of the client relationship. When applying the RBA, attorneys and firms should bear in mind that specified activities have been found to be more susceptible to ML/TF activities because they involve the movement or management of client assets; this susceptibility may be heightened when these activities are conducted on a cross-border basis. These specified activities are set out in Schedule 1 of the AML/CFT Act.

Attorneys-at-law should perform a risk assessment of clients at the inception of a client relationship. Such risk assessment may well be informed by findings of the NRA and any other information which may be relevant to assess the risk level particular to their legal practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Attorneys-at-law may also refer to FATF Guidance on indicators and risk factors[2]. During the course of a client relationship, procedures for ongoing monitoring and review of the client/transactional risk profile are also important.

CATEGORIES OF RISK

Attorneys-at-Law s may assess ML/TF risks by applying various categories. This provides a strategy for managing potential risks by enabling Attorneys-at-Law, where required, to subject each client to reasonable and proportionate risk assessment.

The most commonly-used risk categories are:

2 Refer to FATF Guidance for a Risk-Based Approach for Legal Professionals.

a) country or geographic risk;
b) client risk; and
c) risk associated with the particular service offered (Transaction Risk).

The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the Attorney-at-Law and/or accounting firm. These criteria, however, should be considered holistically and not in isolation. Attorneys-at-Law, based on their individual experiences and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

Country or Geographic Risk

Jurisdictions with certain characteristics pose risks. Jurisdictions with AML/CFT regimes that fall below acceptable standards may be regarded as high risk. Jurisdictions which support terrorist activities or are known for significant political corruption are also high risk.
There is no universally agreed definition by competent authorities that prescribes whether a particular country or geographic area (including the country within which the Attorney-at-Law practices) represents a higher risk. Country risk, in conjunction with other risk factors, provides useful information on ML/TF risks.

Geographic risks of ML/TF may arise in a variety of circumstances, including from the domicile of the client, the location of the transaction or the source of wealth or the funds. Attorneys-at-Law should be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting business from such countries. Attorneys-at-law should observe the Public Statements issued by the FATF and CFATF as it relates to business relationships and transactions with natural and legal persons, from listed countries and to observe the list of countries published by any competent authority which lists countries that are non-compliant or do not sufficiently comply with FATF recommendations.

Attorneys-at-law should therefore have regard to where a transaction or request for their services originated, but also whether a high-risk jurisdiction is an intermediate stage in the financing or ownership arrangement.

See Also, *Guideline related to High Risk Customers* issued by the Financial Intelligence Unit Guideline No. 3 of 2021 - https://fiu.gov.gy/wp-content/uploads/2022/12/High-Risk-Customers-Guidelines-No.-3-of-2021.pdf

Client Risk

Determining the potential ML/TF risks posed by a client or category of clients is critical to the development and implementation of an overall risk-based framework. Based on their own criteria, accounting firms and Attorneys-at-Law should seek to determine whether a particular client poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment.

There are several issues that may point to a high risk client, including:

- Industries or sectors where opportunities for ML/TF are particularly prevalent.
- The structure or nature of the entity or relationship makes it difficult to identify the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions.
- PEPs and/or their family members and close associates.
- Companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.
- Cash intensive businesses including money transfer services, casinos and other gaming institutions, dealers in precious metals and non-profit or charitable organizations, where such clients are themselves subject to and regulated for a full range of AML/CFT requirements consistent with the FATF Recommendations, this will aid to mitigate the risks.
- Reluctance to provide relevant information or the Attorney-at-Law having reasonable grounds to suspect that the information provided is incorrect or insufficient.

Transaction Risk

An overall risk assessment of clients should also include determining the potential risks presented by the services being offered by Attorneys-at-Law, who provide a broad and diverse range of services. The context of the services being offered or delivered is fundamental to a RBA. When determining the risks associated with the provision of services related to specified activities, consideration and appropriate weight should be given to transaction risks including:

- Under or over-valued properties. For example, is the property owner selling the property for significantly less than the purchase price? Does the seller seem disinterested in obtaining a better price?
- Use of large amounts of cash. Buyer brings actual cash to the closing. The purchase of a property without a mortgage, where it does not match the characteristics of the buyer. While rules and regulations governing the financial sector are designed to detect situations where large amounts of cash are being introduced, attorneys should keep this factor in mind when evaluating whether a transaction seems suspicious. Property

purchases inconsistent with the individual's occupation or income. Is the property being purchased significantly beyond the purchaser's means?

- Immediate resale of the property. Especially if the sale entails a significant increase or decrease in the price compared to the prior purchase price, without a reasonable explanation.
- Speed of transaction (without reasonable explanation).
- Unusual source of funding. Example: use of third-party funds to purchase a property where it doesn't make sense, i.e. third-party is not a parent, sibling, etc., use several different sources of funds without logical explanation, funding coming from a business but property not being held in business' name, or purchase of property doesn't match the business' purpose.
- Purchases being made without viewing the property, no interest in the characteristics of the property.
- Any other activities which demonstrate suspicious behavior and do not make professional or commercial sense based on the norms in the industry and the normal course of business.

Mitigation Risk

Attorneys-at-law should implement appropriate measures and controls to mitigate the potential ML/TF risks for those clients that, as the result of a RBA, are determined to be higher risk. These measures should be tailored to the specific risks faced, both to ensure the risk is adequately addressed. Paramount among these measures is the requirement for attorneys and appropriate staff to be adequately trained to identify and detect relevant changes in client activity by reference to risk-based criteria.

The presence of a single risk factor, or even multiple factors, does not necessarily mean that the client is engaging in money laundering or financing terrorism and proliferation activities. Attorney-at-laws should be familiar with these risk factors, and exercise sound judgment based on their knowledge of the relevant industry, and when a combination of these factors truly raises a red flag, know the proper action to take.

In light of this, it is crucial that attorneys-at-law develop a sound risk management policy that they will follow in all transactions. This policy should document what customer information is required to facilitate a transaction. It should also set out in what circumstances business would be declined.

KNOW YOUR CLIENT(KYC) /CUSTOMER DUE DILIGENCE (CDD)

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.

CDD is a critical component of the role all Attorneys-at-law can play in helping to identify and combat money laundering and terrorist and proliferation financing. Knowing one's client does not mean knowing the client's name and address. This can only be satisfied by understanding the client's business and his/her desired relationship with the Attorney-at-Law's professional service.

Attorneys-at-law are required to apply each of the following CDD measures:

(i) identification and verification of the client's identity;

(ii) identification of the beneficial owner and taking reasonable measures to verify the identity of beneficial owner;

(iii) understanding the purpose and nature of the business relationship; and

(iv) on-going due diligence on the relationship

Attorneys-at-law as a reporting entity must identify and verify the identity of customers pursuant to Section 15 of the AMLCFT Act 2009 as amended.

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.

In effecting the due diligence process, attorneys-at-law should:

(i) Whenever possible, require prospective clients to be interviewed in person.

(ii) In verifying client identity, use independent official or other reliable source documents, data or information to verify the identity of the beneficial owner prior to establishing the business relationship. Identification documents which do not bear a photograph or signature and which are easily obtainable (e.g. birth certificate) are not acceptable as the sole means of identification. Verification may involve the use of external electronic databases.

(iii) In instances where original documents are not available, only accept copies that are certified by an approved person. Approved persons should print their name clearly, indicate their position or capacity together with a contact address and phone number;

(iv) If the documents are unfamiliar, take additional measures to verify that they are genuine e.g. contacting the relevant authorities; and

(v) Determine through a risk analysis of the type of applicant and the expected size and activity of the account, the extent and nature of the information required to establish

a relationship. (Examples of documentation for different types of clients are set out in **Appendix 1 – Confirmation of Customer Verification of Identity)**

Generally, funds should not be accepted from prospective clients unless the necessary verification has been completed. However, in exceptional circumstances, verification may be completed after establishment of the business relationship. A reasonable timeline for completing the verification process should be established. If after verification efforts there is still discomfort, a report should be made to the FIU. "Funds", in this regard, **does not refer to an initial consultation fee.**

In cases where red flags are present, the agent should apply increased levels of CDD, which could include the following:

1. Obtain additional information, a driver's license, passport or other reliable identification document, to confirm the true identity of the client.
2. If a legal entity is involved, such as a corporation, take additional measures to identify who actually controls or owns the entity and take risk based measures to verify the identity of the owner. This is commonly referred to as beneficial ownership information.
3. Obtain other appropriate information based on experience and knowledge to understand the client's circumstances and business.

In addition, depending on the size of the firm, it may be appropriate to notify and discuss with senior management the higher risk client or a particular situation that raises red flags, and to monitor the relationship if there are a series of transactions with the client.

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

PERSONAL CLIENTS

Attorneys-at-law should obtain relevant information on the identity of their personal clients and seek to verify the relevant information on a risk basis, through the use of reliable, independent source documents, data or information to prove to their satisfaction that the individual is who that individual claims to be.

The basic information should include:

a) True name and permanent residential address;
b) Valid photo-bearing identification, with unique identifier, (e.g. passport, national identification card, driver's licence);
c) Date and place of birth and nationality (if dual, should be indicated);
d) Occupation and business or principal activity;
e) Contact details e.g. telephone number, fax number and e-mail address;
f) Purpose of the business; and
g) Signature.

Attorneys-at-law should determine the degree of verification to be undertaken on a risk basis. In some instances, verification may be satisfied by maintaining current photo-bearing identification with a unique identifier (e.g. passport, national identification card). Where a customer is unable to produce original documentation needed for identification or verification, copies should be accepted, only if certified.

UNAVAILABILITY OF IDENTITY DOCUMENTS

There may be circumstances where some clients are unable to supply the identity documents. Such clients include the elderly, a minor, the disabled and individuals dependent on the care of others. Attorneys may determine what alternate identity documentation to accept and verification to employ. Where applicable, the following should be among documentation obtained:

a) A letter or statement from a person, that the person is who he/she states;
b) Confirmation of identity from another regulated institution in a jurisdiction with equivalent standards.

CORPORATE CLIENTS

To satisfy itself as to the identity of the client, Attorneys-at-Law should obtain:

a) Name of Corporate entity
b) Principal place of business and registered office;
c) Mailing address;

d) Contact telephone and fax numbers;
e) Identity information on the beneficial owners of the entity. This information should extend to identifying those who ultimately own and control the company and should include anyone who is giving instructions to the agent to act on behalf of the company. However, (i) If the company is publicly listed on a recognized stock exchange and not subject to effective control by a small group of individuals, identification on shareholders is not required; (ii) If the company is a private, identity should be sought on persons with a minimum of 10% shareholding.

f) Identity information on directors and officers who exercise effective control over the business and are in a position to override internal procedures / control mechanisms;

g) Description and nature of business;
h) Certified copy of the certificate of incorporation, organization, registration or continuance, as the case may be, or any other certificate that is evidence of the creation, registration or continuance of the body corporate, society or other legal person as such, officially authenticated where the body corporate, society or other legal person was created in another country;
i) By-laws and any other relevant documents, and any amendments thereto, filed with relevant authority as the case may be;
j) Board resolution authorizing the business activity and conferring authority on signatories to the transaction, where appropriate; and
k) Recent financial information or audited statements, depending on the nature of the transaction.

In addition, Attorneys-at-Law may obtain any other information deemed appropriate. For example, one may also request the financial statements of parent or affiliate companies, or seek evidence that the entity is not in the process of being dissolved or wound-up. One should request this information, particularly for non-resident companies, where the corporate customer has no known track record or it relies on established affiliates for funding.

PARTENERSHIP/UNINCORPORATED BUSINESS

Partnerships and unincorporate businesses should meet the relevant requirements set out for a ***Personal Client*** (Above). Each partner as well as immediate family members with ownership control should be identified. Ownership control exists where a partner or an investor in the business enterprise, or an immediate family member (spouse, child, parent, sibling) has at least ten percent interest in the business, or the power to control the direction of the business. In addition to providing the identification documentation for partners/controllers and authorized signatories, where a formal partnership arrangement exists, the Attorney-at-Law may obtain a mandate from the partnership authorizing the business to be undertaken.

TRUSTS

Trust business is usually regarded as inherently risky because of the confidentiality associated with these entities. To satisfy itself as to the identity of the client, the Attorney-at-Law should obtain:

a) Name of trust;
b) Nature / type of trust;
c) Country of establishment;
d) Identity of the trustee(s), settlor(s), protector(s)/controller(s) or similar person holding power to appoint or remove the trustee and where possible the names or classes of beneficiaries;
e) Identity of person(s) with powers to add beneficiaries, where applicable;
f) Identity of the person providing the funds, if not the ultimate settler;
g) Verify beneficiaries before the first distribution of assets;
h) Verify protectors/controllers at the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice;
i) Ongoing due diligence should be applied in the context of changes in any of the parties to the trust, revision of the trust, addition of funds, investment of trust funds or distribution of trust assets/provision of benefits out of trust assets.
j) Verify the identity of the trust by obtaining a copy of the creating instrument and other amending or supplementing instruments.

PROFESSIONAL SERVICE PROVIDERS

Professional service providers act as intermediaries between clients and the professionals providing services to those clients. They include lawyers, accountants and other third parties that act as financial liaisons for their clients.

When establishing and maintaining relationships with professional service providers, Attorneys-at-Law should:

(i) Adequately assess any risk and monitor the relationship for suspicious or unusual activity;
(ii) Understand the intended business, including the anticipated transaction volume, and geographic locations involved in the relationship; and
(iii) Obtain the identity of the beneficial owners of the client funds where it is not satisfied that the intermediary has in place due diligence procedures equivalent to the standard of this Guideline.

POLITICALLY EXPOSED PERSONS (PEPs)

Concerns about the abuse of power by public officials for their own enrichment and the associated reputation and legal risks which Attorneys-at-Law who deal with them may face, have led to calls for enhanced due diligence on such persons. The Financial Action Task Force (FATF) categorizes PEPs as foreign, domestic, or a person who is or has been entrusted with the prominent function by an international organization.

These categories of PEPS are defined as follows:

- Foreign PEPs: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- Domestic PEPs: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- International organization PEPs: persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.
- Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.
- Close associates

See FATF Guidance on Politically Exposed Persons (Recommendations 12 and 22) and ***Financial Intelligence Unit Guideline No.3 of 2017- Politically Exposed Persons*** https://fiu.gov.gy/wp-content/uploads/2022/12/Guideline-No.-3-of-2017-Politically-Exposed-Person-Revised.pdf

Attorneys-at-law should, in relation to foreign PEPs (whether as a client/customer or beneficial owner), in addition to performing normal due diligence measures:

a) Have appropriate risk-management systems to determine whether the client or the beneficial owner is a politically exposed person;
b) Take reasonable measures to establish the source of wealth and source of funds; and
c) Conduct enhanced ongoing monitoring of the business relationship

With respect to domestic PEPs or persons who are or have been entrusted with a prominent public function by an international organization, in addition to performing normal due diligence measures, Attorneys-at-Law should:

a) Take reasonable measures to determine whether a client or the beneficial owner is such a person; and
b) In cases of a higher risk business relationship with such persons, apply the measures referred to in paragraphs (b) and (c) above.

However, a domestic PEP is subject to the foreign PEPs requirements if that individual is also a foreign PEP through another prominent public function in another country. The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

REDUCED CLIENT/ CUSTOMER DUE DILIGENCE

Attorneys-at-law may apply reduced due diligence to a client provided they are satisfied that the client is of such a risk level that qualifies for this treatment.

Such circumstances are set out below:
Where an indication to conduct business is made by:

a) An entity licensed under the Financial Institutions Act;
b) An entity registered under the Securities Industry Act
c) An entity licensed under the Insurance Act;
d) An entity licensed under the Cooperatives Societies Act, Friendly Societies Act or New Building Society Act;
e) The Government of Guyana ; or
f) A statutory body.

Where, owing to the perceived risk, reduced due diligence is applied in any circumstance other than those set out in this section, Attorneys-at-Law must first consider and approve this decision. Evidence of this process must be recorded and stored for the statutory period required after the end of the business relationship.

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. However, it may be necessary to retain records, until such time as advised by the FIU or High Court, for a

period exceeding the statutory period, beginning from the date of termination of the last business transaction, where:

(i) There has been a report of suspicious activity; or
(ii) There is an on-going investigation relating to a transaction or client.

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).

Attorneys-at-Law should establish a document retention policy that provides for the maintenance of a broad spectrum of records, including customer identification data, business transaction records, internal and external reporting and training records.

Internal and External Records

Attorneys-at-Law should maintain records related to unusual and suspicious business transactions for no less than 7 years. These include:

a. All reports made by staff to the Compliance Officer;
b. The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made;
c. Consideration of those reports and of any action taken;
d. Reports by the Compliance officer to senior management and board of directors;
e. Reports to the Authority on positive screening results in relation to terrorist financing and the financing of proliferation; and
f. Reports to the Authority on the total amount of frozen assets in relation to terrorist financing and the financing of proliferation.

Training Records

Attorneys-at-law are required to provide training and awareness programmes and to maintain an on-going training programme for themselves and all persons working in their businesses

In order to provide evidence of compliance with **Section 19(d) of the AMLCFT Act 2009** as amended, at a minimum, the following information must be maintained:

a) Details and contents of the training programme attended by practitioners and staff;
b) Names of staff receiving the training;
c) Dates that training sessions were attended or held; and
d) Results of any testing included in the training programmes;

e) An on-going training plan.

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.

COMPLIANCE FUNCTION

Attorneys-at-Law must establish procedures for ensuring compliance with legal requirements as set out in relevant legislation and this Guideline to demonstrate that they are able to identify suspicious activity.

A sole practitioner has the responsibility of personally carrying out all required due diligence activities, unless this function is contracted out. However, the practitioner remains responsible for the compliance function.

With respect to a legal firm, a compliance officer at the level of management must be appointed. This is to ensure that this officer has access to all relevant internal information without having to seek clearance in each case. Where the compliance function is contracted out, the firm remains responsible for the function.

Internal Reporting Procedures

To facilitate the detection of suspicious transactions, Attorneys-at-Law should:

(i) Require clients to declare the source/and or purpose of funds for business transactions in excess of threshold limits, or such lower amount as the practitioner determines, to reasonably ascertain that funds are not the proceeds of criminal activity. **(See Declaration of Source of Funds/Wealth Form)**

(ii) Develop written policies, procedures and processes to provide guidance on the reporting chain and the procedures to follow when identifying and researching unusual transactions and reporting suspicious activities;

(iii) Identify a suitably qualified and experienced person, at management level, to whom unusual and suspicious reports are channelled. The person should have direct access to the appropriate records to determine the basis for reporting the matter to the Authority

(iv) Require staff to document in writing their suspicion about a transaction;

(v) Require documentation of internal enquiries; and

(vi) Keep a record of all reports made to authorities and responses to enquiries made for the statutory period.

Persons operating as sole practitioners are expected to apply these steps to the extent that they are relevant.

REPORTING SUSPICIOUS ACTIVITY

Attorneys-at-law are required under the AMLCFT Act 2009 as amended to report to the Financial Intelligence Unit where the identity of the person involved, the transaction or any other circumstance concerning that transaction lead to the practitioner to have reasonable grounds to suspect that a transaction:

(i) Involves proceeds of crime to which the AML/CFT Act 2009 applies

(ii) Involves the financing of terrorism/ proliferation

(iii) Is of a suspicious or an unusual nature

Attorneys-at-Law are advised to monitor suspicious activity, but there is an obligation to report activity that satisfies the threshold for inconsistency with normal behaviour. After a reasonable time, a transaction, or series of transactions, should be cleared of suspicion, and if this cannot be done with a clear conscience, a report should be made to the FIU.

A Suspicious Transaction Report form should be completed and submitted to the FIU for analysis. Once reported, nothing should be done to indicate to any person that such a report was made. There are legal consequences for tipping off a person that an investigation is about to commence or has commenced or that a report was made to the FIU. Bear in mind that tipping off may be inadvertent and could take place through the loose handling of information.

See ***Financial Intelligence Unit Guideline No. 1 of 2013- Suspicious Transaction Reporting:*** https://fiu.gov.gy/wp-content/uploads/2022/12/Guideline-on-Suspicious-Transaction-Reporting.pdf

Financial Intelligence Unit Guideline No. 1 of 2020- Submitting a Report to the FIU via CASEKONNECT: https://fiu.gov.gy/wp-content/uploads/2022/12/Submitting-a-report-to-the-FIU-via-CaseKonnect-01-02-2020.pdf

RED FLAGS

There are a myriad of ways in which money laundering or terrorism financing may occur. Below is a non–exhaustive list of "Red Flags" that may warrant closer attention.

Financial institutions are encouraged to refer to such organizations as the FATF, Egmont Group and United Nations Office on Drugs and Crime for typology reports and sanitised cases on money laundering and terrorist financing schemes, respectively.

IF THE CLIENT:

- Does not want correspondence sent to home address
- Shows uncommon curiosity about internal systems, controls and policies
- Over justifies or explains the transaction
- Is involved in activity out-of-keeping for that individual or business

IF THE CLIENT:

- Produces seemingly false identification or identification or identification or information to be counterfeited, altered or inaccurate
- **Provides insufficient, false or suspicious information, or information that is difficult or expensive to verify**

ECONOMIC PURPOSE

- Transaction is unnecessarily complex for its stated purpose
- Activity is inconsistent with what would be expected from declared business
- 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.
- Accounts that show virtually no banking activity but are used to receive or pay significant amounts not clearly related to the customer or the customer's business.

CASH TRANSACTIONS

- Client starts conducting frequent cash transactions in large amounts when this has not been a normal activity in the past
- Frequent exchanges small bills for large ones

- Deposits of small amounts of cash on different successive occasions, in such a way that on each occasion the amount is not significant, but combines to total a very large amount (ie. Smurfing)
- Consistently making cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Stated occupation is not in keeping with the level or type of activity (eg. Student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over wide geographic area)
- Unusually large deposits or withdrawals of cash by an individual or legal entity whose apparent business activities are normally carried out using cheques and other monetary instruments.
- Multiple and frequent purchase or sale of foreign currency by a tourist
- Multiple and frequent large withdrawals from an ATM using a local debit card issued by another financial institution
- Multiple and frequent large withdrawals from an ATM using debit or credit card issued by a foreign financial institution

DEPOSIT ACTIVITY

- Account with a large number of small cash deposits and a small number of large cash withdrawals
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly exhibits significant activity
- Reactivated dormant account containing minimal sum suddenly receives a deposit or series of deposits are made to a client's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.

CROSS BORDER TRANSACTIONS

- Deposits followed within a short time by wire transfers to or through locations of concern such as countries known or suspected to facilitate money laundering activities.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system

- Immediate conversions of funds transfers into monetary instruments in the name of third parties.
- Frequent sending and receiving of wire transfers, especially to or from countries considered high risk for money laundering or terrorist financing, or with strict secrecy laws. Added attention should be paid if such operations occur through small or family run banks, shell banks or unknown banks.
- Large incoming or outgoing transfers with instructions for payment in cash
- Client makes frequent or large electronic funds transfers for person who have no account relationship with the institution.
- Client instructs you to transfer funds abroad and to expect an equal incoming transfer
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country
- Wire transfers are received from entities having no apparent business connection with client.

PERSONAL TRANSACTIONS

- Client has no employment history but make frequent large transactions or maintains a large account balance
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount
- Client frequently makes automatic banking machine deposits just below the reporting threshold.
- Increased use of safety deposit boxes. Increased activity by the person holding the boxes. The Depositing and withdrawal of sealed packages.
- Third parties make cash payments or deposit cheques to a client's credit card
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.

CORPORATE AND BUSINESS TRANSACTIONS

- Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which is inconsistent with the client's business.
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity
- Unexplained transactions are repeated between personal and business accounts.
- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is

through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

LENDING

- Customer suddenly repays a problem loan unexpectedly, without indication of the origin of the funds
- Loans guaranteed by third parities with no apparent relation to the customer
- Loans backed by assets, for which the source is unknown or the value has no relation to the situation of the customer.
- Default on credit used for legal trading activities, or transfer of such credits to another company, entity or person, without any apparent justification, leaving the bank to enforce the guarantee backing the credit.
- Use of standby letters of credit to guarantee loans granted by foreign financial institutions, without any apparent economic justification.

SECURITIES

- Client frequently makes large investments in stocks, bonds, investments trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.

ACCOUNTS UNDER INVESTIGATION

- Accounts that are the source or receiver of significant funds related to an account or person under investigation or the subject of legal proceedings in a court or other competent national or foreign authority in connection with fraud, terrorist financing or money laundering.
- Accounts controlled by the signatory of another account that is under investigation or the subject of legal proceedings by a court or other competent national or foreign authority with fraud, terrorist financing or money laundering.

FIDUCIARY BUSINESS

- Client seeks to invest a large sum of money with no apparent interest in the details of the product and does not enquire about the characteristics of the product and or feigns market ignorance
- Corporate client opens account with large sum of money that is not in keeping with the operations of the company, which may itself have recently been formed.

- Formation of a legal person or increases to its capital in the form of non-monetary contributions of real estate, the value of which does not take into account the increase in market value of the properties used.

EMPLOYEES

- Lifestyle, financial status or investment activity is not in keeping with the employee's known income
- Reluctance to go on vacation, to change job position or to accept a promotion, with no clear and reasonable explanation.
- Employee frequently receives gifts/and or invitations from certain clients, with no clear or reasonable justification
- Employee hinders colleagues from dealing with specific client(s) with no apparent justification
- Employee documents or partially supports the information or transactions of a particular client with no clear and reasonable justification
- Employee frequently negotiates exceptions for a particular client(s).

TERRORIST FINANCING INDICATORS

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. Behaviour indicators include:

- 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

PROLIFERATION FINANCING INDICATORS

- When customer is involved in the supply, sale, delivery or purchase of dual-use, proliferation sensitive or military goods, particularly to higher risk jurisdictions.
- When customer or counter-party, or its address, is the same or similar to that of an individual or entity found on publicly available sanctions lists.
- The customer is a research body connected with a higher risk jurisdiction of proliferation concern.
- When customer's activities do not match with the business profile provided to the reporting entity.
- When customer is vague about the ultimate beneficiaries and provides incomplete information or is resistant when requested to provide additional information.
- When customer uses complicated structures to conceal connection of goods imported / exported, for example, uses layered letters of credit, front companies, intermediaries and brokers.
- When a freight forwarding / customs clearing firm being listed as the product's final destination in the trade documents.
- When final destination of goods to be imported / exported is unclear from the trade related documents provided to the reporting entity.
- Project financing and complex loans, where there is a presence of other objective factors such as an unidentified end-user.
- The transaction(s) involve an individual or entity in any country of proliferation concern.
- The transaction(s) related to dual-use, proliferation-sensitive or military goods, whether licensed or not.
- The transaction(s) involve the shipment of goods inconsistent with normal geographical trade patterns i.e. where the country involved does not normally export or import or usually consumed the types of goods concerned.
- Over / under invoice of dual-use, proliferation-sensitive or military goods, trade transactions.
- When goods destination/shipment country is different from the country, where proceeds are sent/ received without any plausible reason.

APPENDICES

APPENDIX 1

CONFIRMATION OF CUSTOMER VERIFICATION OF IDENTITY

Part A - Personal Customers

Full Name of Customer: (Mr/Mrs/Ms)
…….
Known Aliases:……..……
Identification:…….…...
Current Permanent Address:…….
Date of Birth:…… Nationality:…….....
Country of Residence:……
Specimen Customer Signature Attached: **Yes ___ No__**

Part B - Corporate & Other Customers

Full Name of Customer:……
Type of Entity: ……..
Location & domicile of Business: ……
Country of Incorporation: …….
Regulator / Registrar: ……
Names of Directors: ……..
……
Names of majority beneficial owners:……...
……

Part C

We confirm that the customer is known to us. **Yes ___No ____**

We confirm that the identity information is held by us. **Yes___ No ___**

We confirm that the verification of the information meets - the requirements of Guyana's law and AML/CFT/CPF Guideline. **Yes ___ No __**

We confirm that the applicant is acting on his own behalf and - not as a nominee, trustee or in a fiduciary capacity for any - other person. **Yes ____No ___N/A _____**

Part D

Customer Group Name: ……

Relation with Customer: ……...

Part E

Name & Position of Preparing Officer: ……

(*Block Letters*)

Signature & Date:……..

Name & Position of Authorising Officer:……..

(*Block Letters*)

Signature & Date:……..…….

APPENDIX 2

DECLARATION SOURCE OF FUNDS/WEALTH

Customer Name Or Business:……..……..
Current Address:…….
Account Number:…….
Identification:……...
Amount Of Transaction & Currency:

Description/Nature Of Business Transaction:

□ Deposit □ Monetary Instrument □ Currency Exchange □ Wire Transfer □ Credit/ Debit Card
□ ATM □ Loan □ Investment □ Trust Settlement / Distribution □ Other, Please specify _____

Source of Funds / Wealth: …….
Supporting Evidence:……..
Customer Signature:……
Date:……

Transaction Approved? □ YES □ NO

If No, state reason:……..

_____

OFFICER COMPLETING TRANSACTION
(Signature & Title)

_____

AUTHORISING OFFICER

(*Signature & Title*)