ANTI-MONEY LAUNDERING/ COMBATING TERRORIST FINANCING GUIDELINE

For

ATTORNEYS-AT-LAW AND ACCOUNTANTS

Anti-Money Laundering Authority
May, 2016

AML/CFT Guideline for Attorneys-at-Law and Accountants

TABLE OF CONTENTS

AML/CFT Guideline for Attorneys-at-Law and Accountants

ANTI-MONEY LAUNDERING/COMBATING TERRORIST FINANCING

Terms Used In This Guideline

AMLA	Anti-money laundering authority
AML/CFT	Anti-money laundering and counter financing of terrorism
CDD	Customer Due Diligence
DNFBPs	Designated Non-Financial Business Professionals
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Customer
MLFTA	Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23
PEP	Politically Exposed Person

1.0 INTRODUCTION

Experience and careful study have taught that the threats of money laundering and the financing of terrorism extend beyond the traditional financial entities which have been receiving attention for control of these activities. It has, therefore, become necessary for certain Designated Non-Financial Businesses and Professions (DNFBPs) to be regulated so as to keep them safe from these 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.

The entities identified by the principle local legislation as DNFBPs for the purpose of our anti-money laundering and counter financing of terrorism infrastructure as set out in the Second Schedule of the Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 (MLFTA) include:

> "An independent attorney-at-law or accountant engaged in any of the following:
>
> a) the purchase, sale or other disposal of real property;
> b) the management of the money, securities or other assets of a customer;
> c) the management of bank savings or securities accounts;
> d) the organisation of contributions for the creation, operation or management of bodies corporate;
> e) the creation, operation or management of legal persons or arrangements; or
> f) the purchase or sale of business entities.

Although these entities have distinct features, the narrow focus of these provisions justify their place in a common Guideline.

Effective use and enforcement of policies that are directed at deterring money laundering and the financing of terrorism gives authenticity and integrity to those areas in which they are applied. This is beneficial to those particular sectors as well as the entire financial sector.

The MLFTA empowers the Anti-Money Laundering Authority (AMLA), pursuant to section 26, to issue guidelines with respect to these activities. This Guideline is so issued for the guidance of persons and entities operating as attorneys-at-law or accountants in Barbados, when engaged as set out above.

The definitions appearing in the MLFTA apply mutatis mutandis to the Guideline.

Adherence to guidelines issued pursuant to section 26 of the MLFTA is mandatory. It may be noticed, however, that this Guideline contains provisions that are either permissive or advisory, and others that are obligatory. Where action is advised, the enforcing entity is at liberty to apply an alternative course of action, as long as it is equally effective in keeping that entity and the financial system safe.

The essential ingredient in an effective anti-money laundering system is an efficient know your customer due diligence system. Everything in this Guideline is founded on this understanding and is aimed at equipping users of it to apply such measures in their business affairs.

2.0 APPLICATION

This Guideline applies to all persons and entities operating as attorneys-at-law or accountants, whether as business owners or as sole practitioners, when they are performing the functions set out above. It is expected to be followed by principals and their agents.

3.0 MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1 Money Laundering

Money laundering has been defined as the act or attempted act to disguise the source of money or assets derived from criminal activity. It is the effort to transform "dirty" money, into "clean" money. 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.

3.2 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.

As information changes, the United Nations publish lists of terrorist or terrorist organisations. 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 Commissioner of Police.

4.0 LEGISLATIVE AND REGULATORY FRAMEWORK

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

(a) Drug Abuse (Prevention and Control) Act, Cap. 131;
(b) Proceeds of Crime Act, Cap. 143;
(c) Mutual Assistance in Criminal Matters Act, Cap. 140A;
(d) Anti-Terrorism Act, 2002-6;
(e) Anti-Terrorism (Amendment) Act, 2015; and
(f) Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23; and

Section 4 of the MLTFA provides that it applies to the DNFBPs set out in the Second Schedule as it does to financial institutions. This means that the legislative infrastructure which applies to the traditional financial institutions, also applies to the DNFBPs.

The MLFTA indicates that a financial institution engages in money laundering if it fails to take reasonable steps to implement or apply procedures to control or combat money laundering and it confers responsibility for the supervision of financial institutions to the AMLA, which was

established in August 2000. A Financial Intelligence Unit (FIU) has been established to carry out AMLA's supervisory function over financial institutions and DNFBPs.

As the operational arm of the AMLA, the FIU's responsibilities, inter alia, include:

(i) Receiving suspicious or unusual transactions reports from financial institutions;
(ii) Investigating suspicious or unusual transactions reports;
(iii) Instructing supervised entities to take steps that would facilitate an investigation; and
(iv) Providing training in respect of record keeping obligations and reporting obligations under the MLFTA.

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

5.0 GATEKEEPERS

Gate keepers are businesses or professionals that are able to provide access into the financial system. They have the ability to allow illicit funds into the financial system, whether knowingly or not. This informs why it was thought necessary to regulate these activities for anti-money laundering purposes, although they are not financial institutions.

5.1 The Role of The Attorney-at-Law

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 penalties provisions of the MLFTA or the appendix in this Guideline.

The MLFTA 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 AMLA 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.

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.

The legal requirements apply to an independent attorney-at-law as they do to a firm, partnership or corporate arrangement. Therefore, "attorney" means a sole practitioner, partner, or employed professional within a professional firm. It is not meant to 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.

5.2 The Role of The Accountant

Accounting professionals 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 accountants provide may be important to a money laundering enterprise. For example, accounting expertise is needed to set up complex illicit transactions, and to unravel them, especially where organized crime is involved.

Often, fraud and money laundering are carried out by people who know more about the accounting systems and other practices than many auditors or police investigators. Under Barbados' MLFTA, accountants are brought under the umbrella of the anti-money laundering infrastructure in the same way as attorneys-at-law. Accountants too, as DNFBPs, must apply the provisions of the MLFTA in the same way as financial institutions. As is the case with attorneys, accountants must keep client records, conduct know your client due diligence and make suspicious transaction reports to the FIU when there is a need to do so.

The legal requirements apply to an independent accountant. Therefore, "accountant" means a sole practitioner, partner, or employed professional within a professional firm. It is not meant to 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.

6.0 RISK-BASED APPROACH

The MLFTA provides for the application of a risk-based approach to combating money laundering and the financing of terrorism. In this regard, attorneys and accountants 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, service providers should deploy defensive resources only where there is a threat of money laundering of financing of terrorism. 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 and accountants 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 is the natural person who controls or benefits from the assets of the business.

6.1 Types of Risk

Three types of risk that are of particular importance to attorneys-at-law and accountants are re-emphasized to focus attention:

6.1.1 Geographic Risk:

Barbados promotes itself as an important financial centre for business persons from many diverse parts of the world. Our wide spread of double taxation treaties is ample evidence of this. Further, real estate in Barbados is an attractive asset for persons. It is to be expected, therefore, that the services of lawyers and accountants will be in high demand as many millions of dollars pass through this sector every year.

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.

Practitioners should 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.

6.1.2 Client Risk:

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

- Unusual involvement of third parties.
- Titling a residential property in the name of third party; for example, a friend, relative, business associate, or lawyer. Use of legal entities (corporations or partnerships) that obscure the identity of the person who owns or controls them without a legitimate business explanation.
- High-ranking foreign political officials or their family members.
- No known source of legitimate income.
- Lifestyle not consistent with known means.
- Reluctance to, or difficulty communicating pertinent information.

6.1.3 Transaction Risk:

Transaction risks include the following:

- 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, service providers 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.

6.2 Mitigating Risk

The presence of a single risk factor, or even multiple factors, does not necessarily mean that the client is engaging in money laundering activities. The role of the service provider is to 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 service providers should 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.

7.0 KNOW YOUR CLIENT/CUSTOMER DUE DILIGENCE (CDD)

This is a critical component of the role all gate keepers can play in helping to identify and combat money laundering. 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's or accountant's professional service.

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

(i) Whenever possible, require prospective customers 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. Client identity can be verified using a combination of methods such as those listed at Appendix 4. 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. See Appendix 5. 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 4.

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.

7.1 Personal Customer

An attorney-at-law or accountant should obtain relevant information on the identity of his/her client or customer 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 his/her satisfaction that the individual is who that individual claims to be. See Section 2 of the MLFTA. 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.

The practitioner 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 if certified by persons listed in Appendix 5.

7.2 Unavailability of Identity Documents

There may be circumstances where some types of clients or customers are unable to supply the identity documents. Such clients include the elderly, a minor, the disabled and individuals dependent on the care of others. Practitioners 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 listed at Appendix 5 that the person is who he/she states;
b) Confirmation of identity from another regulated institution in a jurisdiction with equivalent standards;

7.3 Corporate Client/Customer

To satisfy itself as to the identity of the client, the attorney-at-law or accountant 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 recognised 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, organisation, 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 the Registrar of Corporate Affairs and Intellectual Property, the Financial Services Commission or the Registrar of Friendly Societies, as the case may be;
j) Board resolution authorising 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, the practitioner 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.

7.4 Partnership/Unincorporated Business

Partnerships and unincorporated businesses should meet the relevant requirements set out in Section 6.1. 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 authorised signatories, where a formal partnership arrangement exists, the practitioner may obtain a mandate from the partnership authorising the business to be undertaken.

7.5 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 or accountant 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.

7.6 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, a practitioner 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.

7.7 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 practitioners who deal with them may face, have led to calls for enhanced due diligence on such persons. The Financial Action Task Force (FATF) categorises PEPs as foreign, domestic, or a person who is or has been entrusted with the prominent function by an international organisation. 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 organisation PEPs: persons who are or have been entrusted with a prominent function by an international organisation, 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 are individuals who are closely connected to a PEP, either socially or professionally.

1) Practitioners 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.

2) 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, practitioners 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.

7.8 Reduced Client/Customer Due Diligence

An attorney-at-law or accountant may apply reduced due diligence to a client provided he/she is 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 International Financial Services Act or the Financial Institutions Act;
b) An entity registered under the Securities Act or the Mutual Funds Act;
c) An entity licensed under the Insurance Act or Exempt Insurance Act;
d) An entity licensed under the Cooperatives Society Act, Friendly Societies Act or Building Societies Act;
e) The Government of Barbados; 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, senior management 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.

8.0 RECORD-KEEPING

To demonstrate compliance with the MLFTA and to allow for timely access to records by the FIU, practitioners 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. Business transaction records should be maintained for a minimum of five years in accordance with section 18 of the MLFTA. 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.

8.1 Training Records

Practitioners 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 21 of the MLFTA, 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.

9.0 COMPLIANCE FUNCTION

Practitioners 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 or accounting 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.

9.1 Internal Reporting Procedures

To facilitate the detection of suspicious transactions, a practitioners should:

(i) Require clients or customers 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. Appendix 7 indicates a specimen of a Declaration Source of Funds (DSOF) form. Where electronic reports are employed instead of the form, they should capture the information included on the Appendix and should be signed by the customer;
(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.

9.2 External Reporting - Reporting Suspicious Activity

Practitioners are required by law to report forthwith to the FIU where the identity of the person involved, the transaction or any other circumstance concerning that transaction lead the practitioner to have reasonable grounds to suspect that a transaction:

(i) Involves proceeds of crime to which the MLFTA applies;
(ii) Involves the financing of terrorism; or
(iii) Is of a suspicious or an unusual nature.

Attorneys-at-law and accountants 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.

APPENDICES

APPENDIX 1

Summary of Money Laundering and Terrorism Sanctions and Offences

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
Reporting Obligations	Failure to make a report on a transaction involving proceeds of crime, the financing of terrorism or is of a suspicious or unusual nature to the FIU Director.	$100,000 on directors jointly and severally and /or 5 years imprisonment	Section 23 (2) MLFTA
	Failure to maintain business transactions records.	$100,000 on directors jointly and severally	Section 18(4) MLFTA
	Failure of a person to report transfers out of Barbados or transfers Barbadian currency or foreign currency into Barbados, of more than BDS$10,000 without Exchange Control permission.	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 24(6) MLFTA
	Failure by a person to report receiving more than BDS$10,000 in Barbadian currency (or foreign equivalent) without the Exchange Control permission.	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 24 (6) MLFTA
Internal Policies, procedures, controls; Internal reporting procedures; Internal employee training and awareness programs	Failure to develop policies and procedures; audit functions; and procedures to audit compliance.	Imposition of a pecuniary penalty (up to $5,000 for any of the circumstances referred to at section 34(1) of the MLFTA; $500 daily for failure to take a measure or action or cease a behaviour or practice) in accordance with section 36.	Section 19(2) of the MLFTA

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
Information Gathering & Investigations	Failure to comply with any instruction issued or request made by the FIU Director.	The licence of the financial institution may be suspended.	Section 30(5) of the MLFTA.
Onsite Inspections	Failure to comply with an instruction or request made by an authorised officer or Regulatory Authority.	The licence of the financial institution may be suspended.	Section 31(4) of the MLFTA
Interference in the Line of Duty	The obstruction, hindrance, molestation or assault to any member of the Authority, constable or other person in performing duties under the Act.	$50,000 or imprisonment of 2 years or both.	Section 42 MLFTA
Directives	Contravention of the Act but circumstances do not justify taking action under sections 34, 35 or 36 of the MLFTA.	Issuance of directives by the Anti-Money Laundering Authority or Regulatory Authority to cease and desist.	Section 33 of the MLFTA.
Money Laundering Offences	Engagement in money laundering.	Summary conviction - $200,000 or 5 years imprisonment or both. Conviction on indictment - $2,000,000 or 25 years imprisonment or both. Forfeiture of licence for financial institution.	Section 6 (1) MLFTA Sections 35 & 46(1)
	Providing assistance to engage in money laundering.	Summary conviction - $150,000 or 4 years imprisonment or both. Conviction on indictment - $1,500,000 or 15 years imprisonment or both	Section 6(2) MLFTA

Area	Description of Offence / Breach	Description of Fine/Sanction	Section of Legislation
	A body of persons (corporate or unincorporated) whether as a director, manager, secretary or other similar officer engaging in a money laundering offence.	Subject to trial and punishment accordingly.	Section 44 MLFTA
Disclosure of Information	Disclosure of information on a pending money laundering investigation. Falsifying, concealing, destruction or disposal of information material to investigation or order.	$50,000 or 2 years imprisonment or both	Section 43(b) MLFTA
	Disclosure or publication of the contents of any document, communication or information in the course of duties under this Act.	$50,000 or 5 years imprisonment or both.	Section 48(3) MLFTA.
Terrorism Offences	Provision or collection funds or financial services to persons to be used to carry out an offence as defined in the listed treaties[1] or any other act.	Conviction on indictment to 25 years imprisonment.	Section 4(1) Anti-Terrorism Act
	Provision of assistance or involve in the conspiracy to commit a terrorist offence.	Conviction on indictment and principal offender punished accordingly.	Section 3 of ATA
	A terrorist offence committed by a person responsible for the management or control of an entity located or registered in Barbados, or otherwise organised under the laws of Barbados.	$2,000,000 notwithstanding that any criminal liability has been incurred by an individual directly involved in the commission of the offence or any civil or administrative sanction as imposed by law.	Section 5 of ATA

[1] Treaties respecting Terrorism: Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents, International Convention against the taking of Hostages, Convention on the Physical Protection of Nuclear Material, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention for the suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf and the International Convention for the Suppression of Terrorists Bombings.

APPENDIX 2

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 organisations 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. In addition, General

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 that appears 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. (i.e. "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 (e.g. a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

 Unusually large deposits or withdrawals of cash by an individual or a 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 a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
 Multiple 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 persons 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 makes 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 parties 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 Dealers

 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 (e.g. mutual fund) 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 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 &/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).

APPENDIX 3

Verification Examples

A. Personal Clients

- Confirm the date of birth from an official document (e.g. birth certificate).
- Confirm the permanent address (e.g. utility bill, tax assessment, bank statement, letter from a public notary).
- Contact the customer e.g. by telephone, letter, email to confirm information supplied
- Confirming the validity of the official documents provided through certification by an authorised person.
- Confirm the permanent and/ business residence through credit agencies, home visits
- Obtain personal references from third parties and existing customers in writing.
- Contact issuers of references.
- Confirmation of employment.

B. Corporate Customers & Partnerships

- Review of current audited information (preferably audited).
- Obtain statements of affairs, bank statements, confirmation of net worth from reputable financial advisers.
- Seek confirmation from a reputable service provider(s).
- Confirm that the company is in good standing.
- Undertake enquiries using public and private databases.
- Obtain prior banking and commercial references, in writing.
- Contact issuers of references.
- Onsite visitations.
- Contact the customer e.g. by telephone, letter, email to confirm information supplied.

C. **Trusts and Fiduciary Clients**

- Seek confirmation from a reputable service provider(s).
- Obtain prior bank references.
- Access public or private databases.

APPENDIX 4

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 Barbados law and AML/CFT 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 5

Approved Persons For Certification of Customer Information

In keeping with Section 7.4.3 on non face-to-face customers, licensees should only accept customer information that has been certified by:

Any of the below persons in Barbados, or their counterparts in jurisdictions with at least equivalent AML/CFT standards:

- Notary Public
- *Senior Public Servant
- Member of the Judiciary
- Magistrate
- Attorney-At-Law with a valid practising certificate
- Accountant who is a member of a national professional association
- Senior banking officer (at least management level)
- Senior Officer of a Consulate/Embassy/High Commission of the country issuing the passport

*In Barbados, this refers to the:

- Registrar/Deputy Registrar of Corporate Affairs and Intellectual Property
- Registrar/Deputy Registrar, Supreme Court
- Registrar/Deputy Registrar, Land Registry
- Chief Personnel Officer, Personnel Administration Division
- Permanent Secretary, Ministry of Home Affairs
- Permanent Secretary, Chief of Protocol, Ministry of Foreign Affairs
- Chief/Deputy Chief Immigration Officer
- Private Secretary to the Governor General
- Commissioner/Deputy Commissioner/Assistant Commissioner/Senior Superintendent of Police
- Superintendent/Assistant Superintendent of Prisons

APPENDIX 6

Suspicious Transaction Report Form

CONFIDENTIAL

SUSPICIOUS/UNUSUAL TRANSACTION REPORT

PLEASE TYPE INFORMATION OR WRITE IN BLOCK LETTERS

IMPORTANT: Complete using information obtained during normal course of the transaction. The report should be completed as soon as practicable AFTER the dealing, and a copy forwarded to:

THE DIRECTOR, FINANCIAL INTELLIGENCE UNIT
ANTI-MONEY LAUNDERING AUTHORITY
P.O. BOX 1372 Bridgetown, Barbados
FACSIMILE NO. (246) 436-4756
Email: **amla@sunbeach.net**
For urgent reporting – Tel. (246) 436-4734/5

FOR OFFICIAL USE ONLY **FIU Reference No.: ……**

PART A – Initial Information

1. ☐ Completed Transaction ☐ Attempted/Aborted Transaction

2. Is this report a correction or follow-up to a Report previously submitted?

☐ NO
(Skip to No.4)

☐ YES
☐ Correction
☐ Follow-up

3. If yes, original Report's date ___ ___ ___ (D M Y)

4. Reporting date ___ ___ ___ (D M Y)

5. Which one of the following reporting entities best describes you:-

- ☐ Accountant
- ☐ Attorney-at-Law
- ☐ Bank
- ☐ Cooperative Society
- ☐ Credit Union
- ☐ Corporate &/or Trust Service Provider
- ☐ Dealer in Precious Metals &/ or Stones
- ☐ Finance Company
- ☐ Gaming Institution
- ☐ General Insurance Company
- ☐ International/Offshore Bank
- ☐ Life Insurance Broker/Agent
- ☐ Life Insurance Company
- ☐ Merchant Bank
- ☐ Money Service Business/Money or Value Transmission Services
- ☐ Mutual Fund Administrator/Manager
- ☐ Real Estate Agent
- ☐ Regulator
- ☐ Securities Dealer
- ☐ Trust Company/Corporation
- ☐ Other ……..

Part B – Identity of Customer 1

1. …… Surname
2. ……... Given Name
3. ……. Middle Name(s)

4. …….. Alternative Names/Spelling
5. …… …… Address(es)

6. ……..... Nationality/(ies)
7. …… Date of Birth (D/M/Y)

8. Identifier #1
   - ☐ ID Card
   - ☐ Passport
   - ☐ Driver's License
   - ☐ Other……
9. ……. ID No.(1)
10. ……. Place of Issue

11. Identifier #2
    - ☐ ID Card
    - ☐ Passport
    - ☐ Driver's License
    - ☐ Other …….
12. ……. ID No.(2)
13. ……. Place of Issue

14. ……. Occupation
15. …….. Employer

16. ……. ……
Telephone # (Include area Code) (H) Telephone # (Include area code) (W)

……. .
Telephone # (Include area Code) (C)

17. ……. ……
Email Address(es) Email address(es)

18. …….. ☐ Personal
Account Number(s) ☐ Corporate
☐ Trust
☐ Other ……..

19. …….
State if account is joint, other signatories, etc

20. …….
Provide other account(s) customer may have at institution, include account type, whether joint, other signatories, etc.

CUSTOMER 2

1. …….. 2. …… 3. …….
Surname Given Name Middle Name(s)

4. ……. 5. ……
Alternative names/Spelling

……
Address(es)

6. ……. 7. ……
Nationality/(ies) Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card 9. ……
☐ Passport ID No.(1)
☐ Driver's License 10. …….
☐ Other ……. Place of Issue

11. Identifier #2 ☐ ID Card
☐ Passport
☐ Driver's License
☐ Other ……

12. …….
ID No.(2)

13. ……
Place of Issue

14. …….
Occupation

15. ……..
Employer

16. …….
Telephone # (Include area Code) (H)

……..
Telephone # (Include area code) (W)

…….
Telephone # (Include area Code) (C)

……..

17. …….
Email Address(es)

…….
Email address(es)

18. ……..
Account Number(s)

☐ Personal
☐ Corporate
☐ Trust
☐ Other ……..

19. ……
State if account is joint, other signatories, etc

20. …….
Provide other account(s) customer may have at institution, include account type, whether joint, other signatories, etc.

Customer 2 applies where there is a transfer between customers.

PART C – To be completed only if the transaction was conducted on behalf of another person/entity other than those mentioned in Part B.

1. ……..
Surname

2. ……..
Given Name

3. …….
Middle Name(s)

4. …….
Alternative- Entity's name

5. ……

……
Address(es)

6. ……. 7. ……
Nationality/(ies) Date of Birth (D/M/Y)

8. Identifier #1 ☐ ID Card ☐ Certificate of Incorporation
☐ Passport ☐ Registration for Business Name
☐ Driver's License
☐ Other ……

9. …….. 10. …….. 11. ……
ID No.(1) Place of Issue Occupation/Type of Business

12. ……... 13. ……. ……...
Employer Telephone (#1)- area code (H) Telephone (#2) - area code (W)

……
Telephone (#3)- area code (C)

14. …….. ……
Email Address #1 Email Address #2

15. ……
Account Number(s)

16. …….
State if a/c joint, other signatories, etc

PART D – Transaction Details

1. Type of Transaction

☐ Cash Out
☐ Deposit to an account Cash/Cheque
☐ Life Insurance Policy purchased/deposit
☐ Purchase of bank draft
☐ Purchase of Jewelry
☐ Purchase of precious metals/stones
☐ Purchase of Gold
☐ Real Estate Purchase ☐ Securities
☐ Conducted Currency Exchange
☐ Inter-account transfer
☐ Outgoing electronic funds transfer
☐ Purchase of diamonds
☐ Purchase of money order
☐ Purchase of traveller's cheques
☐ Other ……

2. Date(s) of transaction(s) | | | |
D M Y

3. …….
Amount & Currency

4. ……..
BBD $ Equivalent

5. …….
Name of drawer/Ordering Customer

6. ……..
Name of Payee/beneficiary

7. …….
Other bank involved, other Country

Please provide copies of relevant documents (e.g. bank statements, real estate documents, etc.) for suspicious or unusual activity and identification and verification information.

PART E – Grounds for Suspicion

(Please describe clearly and completely the factors or unusual circumstances that led you to suspect that the transaction(s) involve(s) the proceeds of crime, involve(s) the financing of terrorism, is of a suspicious or unusual nature.)

If the report relates to attempted transaction(s), describe why each one was not completed.

……..
……
……
……
……
……
……
……
……
……
……
……

……

……

(If insufficient space, please attach a separate sheet.)

PART E2

If additional information is attached, please tick box ☐

PART E3

If identity of the customer has not been established in PART B and they are not known to the officer, give a description (e.g., sex, approximate age, height, built, ethnicity, complexion, etc.)

……

……

……

……

……

……

……

PART F - Details of financial institution/place of transaction

1. …… Organisation

2. …….. Branch where transaction occurred if applicable

3. ……. Name and Title of Reporting Officer

4. ……. Signature of Reporting Officer

5. …….. Dealers internal reference number

6. …….. Reporting Officer‘s direct telephone number

APPENDIX 7

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 □ (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*)