



ANTI-MONEY LAUNDERING/ COMBATING TERRORIST FINANCING GUIDELINE

**For
Financial Institutions Regulated by the
Financial Services Commission**

**ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013**



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Table of Contents

EXECUTIVE SUMMARY	5
INTERNATIONAL INITIATIVES	6
INTERPRETATION	7
1.0 INTRODUCTION	12
2.0 APPLICATION	13
3.0 MONEY LAUNDERING AND FINANCING OF TERRORISM	13
3.1 Money Laundering	13
3.2 Financing of Terrorism	13
4.0 LEGISLATIVE AND REGULATORY FRAMEWORK	14
5.0 THE ROLE OF THE BOARD AND SENIOR MANAGEMENT	15
5.1 Risk-Based Approach	17
6.0 CUSTOMER DUE DILIGENCE	19
6.1 Personal Customer	23
6.1.1 Unavailability of Identity Documents	23
6.2 Corporate Customer	24
6.3 Partnership/Unincorporated Business	25
6.4 Enhanced Due Diligence	25
6.4.1 Trust Clients	26
6.4.2 Non-Profit Organisations (NPOs)	27
6.4.3 Non Face-to-Face Customers	28
6.4.4 Introduced Business	29
6.4.5 Professional Service Providers	30
6.4.6 Politically Exposed Persons (PEPs)	31
6.4.7 Corporate Vehicles	32
6.5 Non-Simplified Due Diligence for Higher Risk Scenarios	33
6.6 Higher Risk Scenarios	33
6.7 Retrospective Due Diligence	33
6.8 Reduced Customer Due Diligence	34



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

7.0 UNUSUAL AND SUSPICIOUS TRANSACTIONS	35
7.1 Internal Reporting Procedures	36
7.2 External Reporting	37
8.0 COMPLIANCE AND AUDIT	38
9.0 RECORD-KEEPING	39
9.1 Internal and External Records	40
9.2 Training Records	41
10.0 TRAINING AND AWARENESS	41
10.1 Content and Scope of the Training Programme	42
11.0 PRE-EMPLOYMENT BACKGROUND SCREENING	43
12.0 SECTOR-SPECIFIC GUIDANCE	44
12.1 Insurance	44
12.2 Mutual Funds and Mutual Fund Administrators	46
12.2.1 Timing of Verification	47
12.2.2 Assumed Business	48
12.2.3 Fund Compliance Procedures	48
12.3 Market Actors: Securities and Investment Business	50
12.3.1 Client Verification	51
12.3.2 Enhanced Due Diligence, Warning Flags and Suspicious Transactions	52
APPENDICES	
1. Coverage of Activities of Financial Institution	55
2. Additional References	56
3. (a) Summary of Money Laundering and Terrorism Sanctions and Offences	57
(b) Summary of Administrative Sanctions	60
4. Verification Examples	61
5. Approved Persons for Certification of Customer Information	62
6. Confirmation of Customer Verification of Identity	63
7. Red Flags	65
8. Declaration Source of Funds/Wealth	70



AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

9. Suspicious/Unusual Transaction Report 71



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

GUIDANCE NOTE ON ANTI-MONEY LAUNDERING/COMBATING TERRORIST FINANCING

EXECUTIVE SUMMARY

This document serves as a guide on regulations and codes of practice as mandated under the Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23 (MLFTA). The document contains sufficiently detailed guidance for an approach to guidelines related to customer due diligence for the non-bank financial sector. Furthermore, it is expected to provide the industry with some degree of clarity of what will be expected and how key aspects of the regulatory regime fit together. Under the MLFTA, reporting entities have a range of responsibilities, including:

- a. Developing and maintaining a risk assessment and risk-based anti-money laundering and the combating of the financing of terrorism (AML/CFT) programme;
- b. Customer identification and identity verification;
- c. Ongoing customer due diligence;
- d. Suspicious transaction reporting;
- e. Record keeping;
- f. Auditing and annual reporting.

The risk-based approach which is discussed more thoroughly in later sections underpins the current regulatory regime. Financial institutions are expected to make decisions about how to manage and mitigate money laundering and terrorist financing risks according to the size, nature and complexity of the organization.

An AML/CFT programme sets out the internal policies, procedures and controls necessary to detect money laundering and financing of terrorism and to manage and mitigate the risk of it occurring. For the purposes of this guideline:

- policies set out expectations, standards and behaviour in a business;
- procedures are more detailed and set out day-to-day operations; and
- controls are tools that management use to ensure the business complies with policies and procedures.

The policies, procedures and controls that are implemented must be adequate and effective. They must be sufficiently robust to reasonably address the risks outlined in a registered entity's risk assessment. For example, if a financial institution rated a particular type of customer as "high risk" in the risk assessment, then your AML/CFT programme should reflect this risk rating with adequate and effective policies, procedures and controls. This should include a policy to conduct enhanced due diligence on such customers, the procedures for doing so and the controls necessary to ensure that the appropriate treatment



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

follows.

The MLFTA requires reporting entities to develop a risk assessment and compliance programme that describes policies, procedures and controls aimed at meeting minimum requirements, and that adequately manages and mitigates the risks of money laundering and financing of terrorism. A risk-based approach offers flexibility to reporting entities to respond proportionately to identified risks. Well-targeted and prioritized anti-money laundering programme will deter money laundering and financing of terrorism activity.

This guideline is used to provide the industry with benchmarks for the proper functioning of their operations, and will be referenced by the FSC in the conduct of its supervisory role. Furthermore, guidance will assist reporting entities in determining how they may deal with meeting their obligations under the MLFTA. For the regulator, guidelines may be applied either universally or on a sector-specific basis. Managing consistency between sectors and ensuring there are no money laundering or terrorist financing vulnerabilities is important. The document includes content for specific guidance which will be broadly consistent across sectors, and where appropriate, sector-specific guidance is provided.

INTERNATIONAL INITIATIVES

The Financial Action Task Force (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 FATF normally issues Guidance and Best Practices Papers to assist countries in implementing the Recommendations. The growing body of work includes Guidance on *Politically Exposed Persons* and *Risk-Based Approach to Combatting Money Laundering and Terrorist Financing*. Financial institutions should keep abreast of developments in the international standard and refine their programmes accordingly.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

INTERPRETATION

In the AML/CFT Guideline, unless otherwise stated:

"account" means any facility or arrangement by which a financial institution does one or more of the following:

- (a) accepts deposits of currency;
- (b) allows withdrawals of currency or transfers of currency between accounts;
- (c) pays cheques or payment orders drawn on a financial institution by, or collects cheques or payment orders on behalf of a person;
- (d) supplies a safety deposit box;

"authorised officer" means a person authorised to conduct an inspection pursuant to section 31 (1) of the MLFTA.

"Authority" means the Anti-Money Laundering Authority appointed by the Minister;

"benefit" has the meaning assigned to it by section 4 of the Proceeds of Crime Act;

"business arrangement"

(a) means an arrangement, between 2 or more parties, the purpose of which is to facilitate a financial or other relevant transaction between the parties; and

(b) includes

- (i) any related transaction between any of the parties and another person;
- (ii) the making of a gift; and
- (iii) the opening of an account;

"business transaction" includes a business arrangement and an occasional transaction;

"business transaction record" includes

- (a) the identification records of parties to a business transaction and parties on whose



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

behalf or for whose ultimate benefit a transaction is conducted;

- (b) the method used by a financial institution to verify the identity of the parties referred to in paragraph (a);
- (c) the date of the transaction;
- (d) a description of the transaction sufficient to identify the nature, purpose and method of execution of the transaction;
- (e) the total value of the transaction including the type and amount of currency involved;
- (f) where the transaction involves a negotiable instrument, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee, if any, the amount and date of the instrument, the number, if any, of the instrument and details of any endorsements appearing on the instrument;
- (g) the type and identifying number of any account with the financial institution involved in the transaction;
- (h) the details of any account used for the transaction including bank, branch and sort code;
- (i) account files in respect of the transaction;
- (j) business correspondence in respect of the transaction; and
- (k) the name and address of the financial institution and of the officer, employee or agent of the financial institution who prepared the record;

"Commissioner" means the Commissioner of Police;

"Court" means the High Court;

"customer" means a person who

- (a) seeks to enter or enters into a business arrangement with a financial institution; or
- (b) seeks to conduct or conducts an occasional transaction with a financial institution;

"customer identification data" includes an identification record;

"Director" means the Director of the Financial Intelligence Unit;

"document" means any record of information and includes:



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- (a) anything on which there is writing;
- (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them;
- (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and
- (d) a map, plan, drawing or photograph;

"financial institution" means

- (a) a person who conducts as a business one or more of the activities listed in the First Schedule of the MLFTA and includes:
 - (i) a person who engages in relevant insurance business;
 - (ii) a market actor, self-regulatory organisation, participant and issuer of securities within the meaning of the Securities Act;
 - (iii) a mutual fund and mutual fund administrator within the meaning of the Mutual Funds Act or any person who manages a mutual fund; and
 - (iv) ;
 - (v) a credit union within the meaning of the FSC Act

"financing of terrorism" means an offence set out in section 4 of the Anti-Terrorism Act;

"freeze" means to restrain any transaction in respect of or dealing in property;

"identification record" means:

- (a) in the case of a body corporate, society or other legal person
 - (i) certified copies 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, and any other relevant documents, and any amendments thereto, filed with the Registrar of Corporate Affairs and Intellectual Property, the Registrar of Co-operatives or the Registrar of Friendly Societies, as the case may be; and



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013**

(ii) the name, address, nationality, occupation and business or principal activity, as the case may be, of the directors, shareholders, managers and members of the body corporate, society or other legal person, as the case may be, and such other evidence as may satisfy a financial institution that those persons are the persons they claim to be; and

(b) in the case of an individual, the name, address, nationality, occupation and business or principal activity, as the case may be, of the individual and such other evidence as may satisfy a financial institution that the individual is who the individual claims to be;

"licence" includes a certificate of registration or similar document issued by a regulatory entity;

"Minister" means the Attorney-General;

"money or value transmission service" means the business of accepting cash, cheques or any other monetary instrument or other means of storing value and paying a corresponding sum in cash or in another form to a beneficiary, by means of a communication, message or transfer or through a clearing system to which the money or value transmission service belongs;

"non-financial business entity or professional" means an entity referred to in the Second Schedule of the MLFTA

"occasional transaction" means a financial or other relevant transaction other than one conducted or to be conducted in the course of an existing business arrangement and includes a wire transfer;

"proceeds of crime" means any property or benefit derived, obtained or realised directly or indirectly by any person from unlawful activity wherever committed and any other property or benefit that is mingled with such property or benefit;

"property" includes money and all other property, real or personal, including things in action and other intangible or incorporeal property wherever situate and includes any interest in such property;

"public authority" means the head of a government department, regulatory authority or other public institution;



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

"regulatory authority" has the meaning assigned to it in Part II of the Third Schedule of the MLFTA

"relevant transaction" means an activity referred to in the Second Schedule of the MLFTA

"transaction" includes an attempted or aborted transaction;

"unlawful activity" means

(a) any activity that by the law of Barbados or any other country is a crime and is punishable by death or imprisonment for a period of not less than 12 months; and

(b) a scheduled offence as defined in section 3 of the Proceeds of Crime Act;

"wire transfer" means a transaction conducted or to be conducted on behalf of a person through a financial institution by electronic means with a view to making an amount of money available to the person or another beneficiary at another financial institution.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

1.0 INTRODUCTION

The global threats of money laundering and the financing of terrorism have led financial sector regulators and financial institutions to strengthen their vigilance in support of the efforts of governments to more easily detect attempts to launder money and finance terrorism and to minimise the possibility that their jurisdictions or institutions become involved. Effective enforcement of policies to deter money laundering and the financing of terrorism must, *inter alia*, enhance the integrity of the financial system and reduce incentives for the commission of crime within Barbados.

The Financial Services Commission (FSC), in furtherance of its responsibility for the supervision of non-bank financial institutions and pursuant to its mandate provided by section 53 (1) (d) of the FSC Act, 2010-21 and section 37 (1) of the MLFTA now issues a guideline to provide guidance to financial institutions on how they can fulfil their obligations in relation to the MLFTA. The "Interpretation" section of this document is not exhaustive, and in general, definitions appearing in the MLFTA apply *mutatis mutandis* to the Guideline.

The development and implementation of effective customer due diligence systems and monitoring mechanisms are essential to help combat money laundering and the financing of terrorism. This guideline sets out the expectations of the FSC in relation to the minimum standards for practices by all financial institutions and, together with the MLFTA, it will form an integral part of the framework used by the FSC in assessing how financial institutions implement their AML/CFT policies.

Section 22 of the MLFTA obligates all financial institutions to comply with this guideline. The guideline contains both advisory and obligatory requirements. Financial institutions are permitted to implement alternative but effective measures where matters are framed in advisory terms. Administrative sanctions for non-compliance with the guideline are found at section 34 of the MLFTA Act and will be enforced pursuant to section 37 (4) of this Act.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

2.0 APPLICATION

This guideline¹ applies to financial institutions as defined in the “Interpretation” section of this guideline. These institutions must ensure that, at a minimum, this guideline is also implemented in their branches and subsidiaries abroad and where permitted in the host country, ensure that these operations apply the higher of local and host standards. In accordance with section 37 of the MLFTA the regulator holds primary responsibility for ensuring compliance with the Act and financial institutions must inform the FSC if the local applicable laws and regulations prohibit the implementation of this Guideline.

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.

¹ For the purposes of this guideline, general references to money laundering should be interpreted as references to money laundering and/or the financing of terrorism.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

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. These include:

- Drug Abuse (Prevention and Control) Act, 1990-14, CAP131;
- Proceeds of Crime Act, 1990-13, CAP143;
- Mutual Assistance in Criminal Matters Act, 1992, CAP140A;
- Anti-Terrorism Act, 2002-6 CAP 158; and
- Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2011-23; and
- Transnational Organised Crime (Prevention and control) Act, 2011-3

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 institutions² to the Authority, which was established in August 2000. A Financial Intelligence Unit (FIU) has been established to conduct the Authority's supervisory function over financial institutions. As the operational arm of the Authority, its responsibilities, inter alia, include:

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

Where a financial institution is uncertain about how to treat an unusual or suspicious transaction, it must speak directly to the FIU for preliminary guidance and then make a report as appropriate. Where the FIU believes on reasonable grounds that a transaction involves the proceeds of crime, the FIU will send a report for further investigation to the Commissioner of Police. In addition, the FSC is required by law to provide any information that it has in its possession, which the FIU deems useful for an investigation that is being conducted for the purposes of the MLFTA.

The FSC will assess and review the AML/CFT framework of financial institutions licenced

² Offences and penalties under the MLFTA are set out in Appendix 3.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

under the Financial Services Commission Act, and their compliance with the MLFTA through offsite and onsite examinations. Where deficiencies are identified in the policy framework or operations of the control framework for managing the financial institution's AML/CFT programme, the FSC will agree with the financial institution on a time period to address the shortcomings. However, if the FSC is concerned by the seriousness of non-compliance and/or the lack of responsiveness to previous findings the FSC may enforce its powers under the Financial Services Commission Act of the MLFTA.

Financial institutions should be mindful of the fact that the FSC is required by law to provide to the FIU any information that it has in its possession which the FIU deems useful for an investigation that is being conducted for the purposes of the MLFTA.

From time to time the FSC, in conjunction with the AMLA, will amend this guideline, but financial institutions must, as part of their risk management practices, stay current with emerging developments as they relate to AML/CFT and upgrade their AML/CFT programme where necessary.

5.0 THE ROLE OF THE BOARD AND SENIOR MANAGEMENT

Financial institutions must see AML/CFT as part of their overall risk management strategy. Money laundering and terrorist financing expose a financial institution to transaction, compliance and reputation risk. For financial institutions convicted of money laundering or terrorist financing, there are considerable costs. Financial institutions must establish an effective AML/CFT programme that minimises these risks and potential costs.

The Board of Directors has ultimate responsibility for the effectiveness of the financial institution's AML/CFT framework. Section 5(2)(b) of the MLFTA establishes that a financial institution engages in money laundering where the financial institution fails to take reasonable steps to implement or apply procedures to control or combat money laundering. The Board has an oversight role designed to ensure inter alia, that there is compliance with all the relevant laws and regulations and international standards. Such compliance must assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

Directors and senior management must be aware that:

- i. The use of a group wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the financial institution and compliant with Barbadian law, regulations and guidelines. Failure to ensure compliance by the financial institution with the requirements of the MLFTA may result in significant penalties for directors and the financial institution (See Appendix 3);
- ii. Subsidiaries and branches of financial institutions including those domiciled outside of Barbados are expected to, at a minimum, comply with the requirements



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

of Barbados MLFTA and this guideline; and

- iii. Where some of a financial institution's operational functions are outsourced, the entity retains full responsibility for compliance with local laws, regulations and guidelines.

Directors must therefore demonstrate their commitment to an effective AML/CFT programme by:

- i. Understanding the statutory duties placed upon them, their staff and the entity itself;
- ii. Approving AML/CFT policies and procedures that are appropriate for the risks faced by the financial institution. Evidence of consideration and approval of these policies must be reflected in the board minutes;
- iii. Appointing an individual within the organisation for ensuring that the financial institution's AML/CFT procedures are being managed effectively; and
- iv. Seeking assurance that the financial institution is in compliance with its statutory responsibilities as it relates to AML/CFT. This includes reviewing the reports from Compliance on the operations and effectiveness of compliance systems. See Section 8.0.

Senior management is responsible for the development of sound risk management programmes and for keeping directors adequately informed about these programmes and their effectiveness. These programmes should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments. These programmes must also be formally documented and irrespective of whether the financial institution receives funds from third parties or not, should at a minimum provide for:

- i. The development of internal policies, procedures and controls for inter alia:
 - a. The opening of customer accounts and verification of customer identity;
 - b. Establishing business relations with third parties (including custodians, fund managers, correspondent banks, business introducers);
 - c. Determining business relationships that the financial institution will not accept;
 - d. The timely detection of unusual and suspicious transactions, and reporting to the Authority;
 - e. Internal reporting; and
 - f. Record retention.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

-
- ii. The recruitment of a level of staff, appropriate to the nature and size of the business, to conduct identification and research of unusual transactions, as well as the reporting of suspicious activities;
 - iii. An ongoing training programme designed to ensure adherence by employees to the legal and internal procedures, and familiarity with the dangers they and the business entity face and on how their job responsibilities can encounter specified money laundering and terrorist financing risks;
 - iv. Designation of a compliance officer at an appropriate level of authority, seniority and independence to coordinate and monitor the compliance program, receive internal reports and issue suspicious transaction reports to the FIU
 - v. Establishment of management information/reporting systems to facilitate aggregate and group wide monitoring;
 - vi. An effective independent risk-based oversight function to test and evaluate the compliance program; and
 - vii. Screening procedures for hiring, and on-going systems to promote high ethical and professional standards to prevent the financial institution from being used for criminal activity.

Policies should be periodically reviewed for consistency with the business model, and product, service offering and a financial institution's risk appetite. Special attention must be paid to new and developing technologies.

5.1 Risk-Based Approach

Other than section 6.8 of this guideline where reduced due diligence may be warranted and some procedures may not be necessary, financial institutions should develop programmes against money laundering and the financing of terrorism. These programmes should include:

- i. The risk rating of customers;
- ii. The development of internal policies, procedures and controls, including appropriate compliance management arrangement, and adequate screening procedures to ensure high standards when hiring employees;
- iii. Record-keeping procedures;
- iv. An appropriate employee education and training programme;
- v. An audit function to test the system; and
- vi. A Know Your Customer (KYC) and customer due diligence process



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Every financial institution is required to develop and implement a risk rating framework which is approved by its Board of Directors as being appropriate for the type of products offered by the financial institution, and capable of assessing the level of potential risk each client relationship poses to the financial institution.

The risk rating framework should include:

- i. The differentiation of client relationships by risk categories (such as high, moderate or low);
- ii. The differentiation of client relationships by risk factors, such as products, client type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size and volume of transactions;
- iii. The type of transactions (e.g. cash transactions, adherence to client activity profile);
- iv. The KYC documentation and due diligence information requirements appropriate for each risk category and risk factor; and
- v. A process for the approval of the downgrading/upgrading of risk ratings.

The FSC recognises the diversity of the institutions it regulates and it will seek to establish that, overall, processes appropriate to institutions are in place and operating effectively. Notwithstanding the risk rating framework highlighted above, all registered entities should therefore design an AML/CFT framework that satisfies the needs of their institution, taking into account:

- i. The nature and scale of the business;
- ii. The complexity, volume and size of transactions;
- iii. The degree of risk associated with each area of operation;
- iv. Type of customer (e.g. whether ownership is highly complex, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group);
- v. Type of product/service (e.g. regular savings, one-off transaction, mortgage, annuity contract, brokerage account);
- vi. Delivery channels (e.g. whether internet business, wire transfers to third parties, remote cash withdrawals);
- vii. Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking or corruption, whether the customer is subject to regulatory or public disclosure requirements); and
- viii. Value of account and frequency of transactions.

In keeping with section 17 of the MLFTA, financial institutions must apply customer due diligence standards on a risk-sensitive basis depending on the type of customer, business



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

relationship or transaction. Reduced due diligence – explained in section 6.8 of this guideline – is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national or institution group systems. Alternatively, financial institutions must apply enhanced due diligence to customers where the risk of being used for money laundering or terrorist financing is high.

Efforts to achieve the above objectives of the MLFTA are likely to be most effective at the point where attempts to launder money first make contact with the overall financial system. There are two issues which follow from this. Firstly, designated bodies who are involved at this "front line" point have a responsibility to be particularly diligent in establishing identity, where appropriate, and being vigilant in relation to suspicious activity. Once past this "front line" point it becomes progressively more difficult for illicit activity to be spotted. Secondly, in the case of designated bodies involved downstream in handling relevant transactions, due recognition may be given to the fact that the person introduced or counterparty has already been identified in accordance with the provisions of this guideline by the introducing designated body. The purpose of this is to avoid unnecessary duplication of effort and recognises that all of an audit trail is unlikely to reside within one designated body alone or is impractical to implement.

In view of the foregoing, financial institutions must document a risk-based approach in their AML/CFT programmes. This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme. This must be evidenced by categorisation of the customer base, products and services by risk rating (e.g. low, medium, and high) and identification of assigned actions by risk types.

While each financial institution will determine the number and name of risk categories, the fundamental issue is for the adoption of reasonable criteria for assessing risks. In addition to "Red Flags" appended to this guideline, typologies of money laundering and terrorist financing schemes are available³ to assist in risk categorisation.

Financial institutions must ensure that systems are in place to periodically test the accuracy of the assignment of the customer base to risk categories and that the requisite due diligence is being followed. In addition, financial institutions must periodically review their risk categories as typologies evolve on practices by money launderers and terrorists.

6.0 CUSTOMER DUE DILIGENCE

Customer due diligence is an essential element of the effort to prevent the financial system

³ For example, www.fatf-gafi.org.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

from being used to perpetrate money laundering and terrorist financing. Financial institutions are ultimately responsible for verifying the identity of their customers. In this regard, financial institutions should not accept anonymous accounts or accounts in fictitious names. If financial institutions maintain numbered accounts, they must ensure compliance with this guideline.

As part of their due diligence process, financial institutions must:

- i. Establish procedures for obtaining identification information on new and existing customers so as to be satisfied that a prospective customer is who he claims to be;
- ii. Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset⁴ of a business relationship. This process must include, where appropriate:
 - a. Taking reasonable measures to understand the ownership and control structure of the customer;
 - b. Obtaining reliable information on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and
 - c. Discontinuing the transaction, if customer documentation information is not forthcoming at the outset in the disclosure of the relationship.
- iii. Employ enhanced due diligence procedures for high risk customers or transactions (Section 6.4);
- iv. Update identification records, on a risk-focussed basis, to ensure that all existing customer records are current and valid and conform to any new requirements (Section 6.7);
- v. Monitor account activity throughout the life of the business relationship in accordance with section 16 of the MLFTA; and
- vi. Review the existing records if there is a material change in how the account is operated or if there are doubts about previously obtained customer identification data.

For the purposes of this guideline, the financial institution must seek to identify the customer and all those who exercise control over the account/transaction. A customer includes:

- i) A person or entity that maintains an account with the financial institution;

⁴ For the purpose of this guideline, the outset of the relationship is the earlier of acceptance of the signed application / proposal, or the first receipt of funds from the customer.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- ii) A person or entity on whose behalf an account is maintained i.e. beneficial owner;
- iii) The beneficiaries of transactions conducted by professional intermediaries such as lawyers, accountants, notaries, business introducers or any other professional service providers; or
- iv) Any person or entity connected with a financial transaction that can pose a significant risk to the financial institution, including persons establishing business relations, purporting to act on behalf of a customer or conducting transactions such as, but not limited to:
 - Opening of deposit accounts;
 - The sale of a life insurance product
 - Entering into fiduciary transactions;
 - Requesting safe custody facilities; and
 - Occasional transactions exceeding thresholds as discussed below or linked transactions under this benchmark.

Section 2 of the MLFTA defines an occasional transaction as a financial or other relevant transaction other than one which is conducted or to be conducted in the course of an existing business arrangement. For the purpose of this guideline, an occasional transaction, such as the exchange of coins for cash is one that is conducted by a person without an account or facility at the financial institution.

Due diligence must be undertaken on, inter alia occasional transactions over BDS\$10,000 or its equivalent in foreign currency, whether conducted in a single or multiple operations that appear to be linked;

The extent of identity information and verification of occasional transactions below these thresholds⁵ is dependent on the materiality of the transaction and the degree of suspicion.

In such circumstances, at a minimum, a financial institution must:

- a. Identify and verify⁶ the persons conducting occasional transactions below the above thresholds;
- b. Maintain an effective system to monitor for abuse of occasional transactions; and
- c. Establish clear instructions for the timely reporting of unusual and suspicious occasional transactions.

⁵ See Section 8.0 for discussion on profiling and transaction limits.

⁶ At a minimum, identification information may consist of the customer's name and address, which is verified by valid photo-bearing ID with a unique identifier.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

In effecting the due diligence process, financial institutions must:

- i) Whenever possible, require prospective customers to be interviewed in person. Exceptions to this are outlined in Sections 6.4.3, 6.4.4 and 6.8;
- ii) In verifying customer identity, use official or other reliable source documents, data or information to verify the identity of the beneficial owner prior to opening the account or 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. Customer 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 must print their name clearly, indicate their position or capacity together with a contact address and phone number and date when the approval was written;
- 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 open an account. Examples of documentation for different types of customers are set out in Sections 6.1 to 6.4.

Generally, financial institutions must not accept funds from prospective customers unless the necessary verification has been completed. In exceptional circumstances, where it would be essential not to interrupt the normal conduct of business (e.g. non face-to-face business and securities transactions), verification may be completed after establishment of the business relationship. However, a reasonable timeline for completing the verification process should be established. Should financial institutions determine this to be an acceptable risk, they must retain control of any funds received until verification requirements have been met. If the requirements are not met, and the financial institution determines that the circumstances give rise to suspicion, it must make a report to the Authority (See Section 7).

Where there is a suspicion that a transaction relates to money laundering or the financing of terrorism, financial institutions should be cognizant of tipping off a customer when conducting due diligence. The financial institution should make a business decision whether to execute the transaction as the case may be, but a suspicious report should be submitted to the Authority.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

6.1 Personal Customer

A financial institution must obtain relevant information on the identity of its customer and seek to verify some of the information on a risk basis, through the use of reliable, independent source documents, data or information to prove to its satisfaction that the individual is who that individual claims to be. See Section 2 of the MLFTA. The basic information must 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, must be indicated);
- d. Occupation;
- e. Contact details e.g. telephone number, fax number and e-mail address;
- f. Purpose of the account; and
- g. Signature.

In addition, the financial institution may obtain any other information deemed appropriate and relevant e.g. source of funds and estimated account turnover.

The financial institution must determine the degree of verification to be undertaken on a risk basis. In some instances, verification may be satisfied by maintaining current government-issued photo-bearing identification with a unique identifier (e.g. passport, or a national identification card).

Where a customer is unable to produce original documentation needed for identification or verification, copies may be accepted if certified by persons listed in **Appendix 5**.

6.1.1 Unavailability of Identity Documents

There may be circumstances where some types of customers are unable to supply the identity documents at Section 6.1. Such customers include the elderly, the disabled, students, minors and individuals dependent on the care of others. Financial institutions must determine what alternate identification documentation to accept and verification to employ. Where applicable, the following must be among documentation obtained:

- a) A letter or statement from a person listed at **Appendix 5** that the person is who he/she states;



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- b) Confirmation of identity from another regulated institution in a jurisdiction with equivalent standards;
- c) Confirmation(s) from the student's workplace, school, college or university; and
- d) Identity information on the adult opening the account, and a birth certificate, or national registration card for the account holder.

6.2 Corporate Customer

To satisfy itself as to the identity of the customer, the financial institution must 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 (See Section 6.1) on the beneficial owners of the entity. This information must extend, as far as practicable, to identifying those who ultimately own and control the company and must include anyone who is giving instructions to the financial institution 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 must be sought on persons with a minimum of 10% shareholding.
- f. Identity information (See Section 6.1) on directors and officers who exercise effective control over the business and are in a position to override internal procedures / control mechanisms and, the signatories to accounts of a financial nature;
- g. Description and nature of business;
- h. Purpose of the account, source of funds and the estimated account activity;
- i. 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;
- j. By-laws and any relevant corporate documents filed with the Registrar of



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Corporate Affairs and Intellectual Property;

- k. Board resolution authorising the opening of the account and conferring authority on signatories to the account; and
- l. Recent financial information or audited statements if applicable.

In addition, the financial institution may obtain any other information deemed appropriate. For example, where it is deemed necessary, a financial institution 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. It should request this information, particularly for non-resident companies, where the corporate customer has no known track record, is not highlighted in section 6.8 of this guideline, or it relies on established affiliates for funding.

6.3 Partnership/Unincorporated Business

Partnerships and unincorporated businesses must meet the relevant requirements set out in Section 6.1. The financial institution must identify each partner as well as immediate family members with ownership control. In addition to providing the identification documentation for partners/controllers and authorised signatories, where a formal partnership arrangement exists, there must be a mandate from the partnership authorising the opening of an account.

6.4 Enhanced Due Diligence

A financial institution may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A financial institution 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 documentation from such countries. Financial institutions must observe the Public Statements issued by the FATF and CFATF as it relates to business relationships and transactions with natural and legal persons, and financial institutions from listed countries.

The financial institution's policy framework must therefore include a description of the types of customers that are likely to pose a higher than average risk and procedures for dealing with such applications. High-risk customers must be approved by senior management and stringent documentation, verification and transaction monitoring procedures must be established. Applying a risk-based approach, enhanced due diligence



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

for high risk accounts may include, where deemed relevant, and with more frequency than applied for low risk customers:

- a) An evaluation of the principals;
- b) A review of current financial statements;
- c) Verification of the source of funds;
- d) Verification of source of wealth;
- e) The conduct of reference checks;
- f) Checks of electronic databases;
- g) Review of relevant country assessment reports; and
- h) Periodic reporting to the Board about high risk accounts.

Types of situations requiring enhanced due diligence are indicated in the subsequent sub-sections.

6.4.1 Trust Clients

Financial institutions must take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction is conducted. This applies especially if there are any doubts as to whether or not these clients or customers are acting on their own behalf.

At a minimum, the financial institution must obtain the following⁷: -

- 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; and
- f. Identity of the person providing the funds, if not the ultimate settlor.

⁷ These minimum requirements apply whether the financial institution is a named trustee or is providing services to a trust.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Depending on the type or nature of the trust, it may be impractical to obtain all of the above at the onset of the relationship e.g. unborn beneficiaries. In such cases, discretion must be exercised and documented in a manner consistent with the requirements in this guideline. In all circumstances, the financial institution must verify beneficiaries before the first distribution of assets. Further, financial institutions must verify protectors/controllers 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.

Ongoing due diligence must 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. Obtaining a copy of the creating instrument and other amending or supplementing instruments satisfies verification of the identity of the trust.

Financial institutions are required to inform the FIU and the FSC when applicable laws and regulations in the domicile where trusts are established, prohibit the implementation of this guideline.

6.4.2 Non-Profit Organisations (NPOs)

NPOs differ in size, income, structure, legal status, membership and scope. They engage in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes or for carrying out other types of "good works". NPOs can range from large regional, national or international charities to community-based self-help groups. They also include research institutes, churches, clubs, and professional associations. They typically depend in whole or in part on charitable donations and voluntary service for support. While terrorist financing may occur through small, non-complex transactions, enhanced due diligence may not be necessary for all clients that are small organisations, dealing with insignificant donations for redistribution among members. Financial institutions must therefore, determine the risk level of activities in which the NPO is engaged.

To assess the risk, a financial institution must focus inter alia on:

- a. Purpose, ideology or philosophy;
- b. Geographic areas served (including headquarters and operational areas);
- c. Organisational structure;
- d. Donor and volunteer base;
- e. Funding and disbursement criteria (including basic beneficiary information);



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- f. Record keeping requirements; and
- g. Its affiliation with other NPOs, Governments or groups.

The financial institution must also include the following in the identity records:

- a) Evidence of registration of the home and local operation, where applicable;
- b) Identity of all signatories to the account; and
- c) Identity of board members and trustees, where applicable.

As part of the verification process, financial institutions must confirm that the organisation is registered under the appropriate laws and with the tax authorities and must carry out due diligence against publicly available terrorist lists. As part of ongoing monitoring activity, financial institutions must examine whether funds are being sent to high-risk countries.

6.4.3 Non Face-to-Face Customers

The rapid growth of financial business by electronic means increases the scope for non-face-to-face business and increases the risk of criminal access to the financial system. Customers may use the Internet, the mail service or alternative means because of their convenience or because they wish to avoid face-to-face contact. Consequently, financial institutions must pay special attention to risks associated with new and developing technologies. Customers may complete applications but financial institutions must satisfy the requirements in this section before establishing a business relationship.

When accepting business from non-face-to-face customers, in order to prove to its satisfaction that the individual is who that individual claims to be, financial institutions shall:

- a. Obtain documents certified by approved persons listed at **Appendix 5**;
- b. Ensure that all company documents are signed by the Company Secretary;
- c. Request additional documents to complement those which are required for face-to-face customers, including more than one photo bearing ID;
- d. Make independent contact with the customer, for example by telephone on a listed business or other number; and
- e. Request third party introduction e.g. by an introducer as noted in Section 6.4.4.

In addition, the financial institution may:



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- a) Carry out employment checks (where applicable) with the customer's consent through a job letter or verbal confirmation on a listed business or other number;
- b) Require the first payment to be carried out through an account in the customer's name with another bank subject to equivalent customer due diligence standards; and
- c) Obtain any other information deemed appropriate.

Where initial checks fail to identify the customer, the financial institution must independently confirm and record additional checks. If the prospective customer is required to attend a branch to conduct the first transaction, or to collect account documentation or credit/debit cards, then valid photo bearing identification must be obtained at that time.

Where a financial institution or its subsidiary initiates transactions in its role as a securities broker or in the sale of mutual funds without establishing face-to-face contact and obtaining all of the relevant documentation, it must make all efforts to obtain such information within a reasonable time. In accepting such transactions, financial institutions must:

- i. Set limits on the number and aggregate value of transactions that can be carried out;
- ii. Indicate to customers that failure to provide the information within the established timeframe, may trigger the termination of the transaction; and
- iii. Consider submitting a suspicious report.

6.4.4 Introduced Business

A financial institution may rely on other regulated third parties to introduce new business in whole or in part but the ultimate responsibility remains with the financial institution for customer identification and verification. Financial institutions must:

- a. Document in a written agreement the respective responsibilities of the two parties;
- b. Satisfy itself that the financial institution or introducer has in place KYC practices at least equivalent to those required by Barbados law and the financial institution itself;
- c. Satisfy itself about the quality and effectiveness of supervision and regulation in the introducer's country of domicile (refer to FATF Recommendations 26, 27 and



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

28); and satisfy itself that the introducer is regulated, and supervised or monitored for, and has measures in place for compliance with CDD and record-keeping requirements in line with the FATF Recommendations¹⁰.

- d. Obtain copies of the due diligence documentation provided to the introducer prior to the commencement of the business relationship;
- e. Satisfy itself that an introducer continues to conform to the criteria set out above (e.g. conduct periodic reviews);
- f. Consider terminating the relationship where an introducer fails to provide the requisite customer identification and verification documents; and
- g. Consider terminating the relationship with an introducer who is not within the financial institution's group, where there are persistent deviations from the written agreement.

When a prospective customer is introduced from within a financial institution's group, provided the identity of the customer has been verified by the introducing regulated parent company, branch, subsidiary or associate in line with the standards set out in the guideline, it is not necessary to re-verify the identification documents unless doubts subsequently arise about the veracity of the information. The financial institution must however, retain copies of the identification records in accordance with the requirements in the MLFTA. Financial institutions must obtain written confirmation from a group member confirming completion of verification. **See Appendix 6.**

6.4.5 Professional Service Providers

Professional service providers act as intermediaries between clients and the financial institution and 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 financial institution must:

- a. Adequately assess account risk and monitor the relationship for suspicious or unusual activity;
- b. Understand the intended use of the account, including the anticipated transaction volume, products and services used, and geographic locations involved in the relationship; and
- c. 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.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Where pooled accounts are managed by:

- a. Providers on behalf of entities such as mutual funds and pension funds; or
- b. Lawyers or stockbrokers representing funds held on deposit or in escrow for several individuals, and funds being held are not co-mingled (i.e. there are sub-accounts), the financial institution must identify each beneficial owner. Where funds are co-mingled, the financial institution must take reasonable measures to identify the beneficial owners. Subject to the FSC's approval, the latter is not required where the provider employs at a minimum, equivalent due diligence standards as set out in this guideline, and has systems and controls to allocate the assets to the relevant beneficiaries. Financial institutions must apply the criteria at Section 6.4.4 in conducting due diligence on providers.

Financial institutions must observe guidance from the FIU regarding attorney-client accounts.

6.4.6 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 financial institutions may face, have led to calls for enhanced due diligence on such persons. The FATF has further categorised the definition of a PEP as either foreign or domestic, and recommends a commensurate level of AML due diligence.

A foreign PEP is an individual who has 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, or important political officials.

Domestic PEPs are individuals who are or who 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, or important political officials.

Also it must be noted that persons who have been entrusted with a prominent function within an international organisation refers to members of senior management such as directors, deputy directors and members of the board or equivalent functions must also be duly considered. The definition of a PEP is not intended to cover middle ranking or more junior individuals in the foregoing categories. However, identifying PEPs can be



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

problematic.

Beneficial owner is defined in the FATF 40 Recommendations to "refer to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement."

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

- i. Have appropriate risk managements systems to determine whether the customer or the beneficial owner is a politically exposed person;
- ii. Obtain senior management approval for the establishing (or continuing, for existing customers) such business relationships;
- iii. Take reasonable measures to establish the source of wealth and source of funds; and
- iv. Conduct enhanced ongoing monitoring of the business relationship.

Financial institutions must take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (ii), (iii) and (iv) above. However, a domestic PEP is subject to the foreign PEP 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 members⁸ or close associates of such PEPs.

6.4.7. Corporate Vehicles

Barbados law prohibits companies from issuing shares in bearer form. Where a financial institution decides that companies with nominee shareholders represent an acceptable business risk, they must exercise care in conducting transactions. Financial institutions must ensure they can identify the beneficial owners of such companies and must immobilise bearer shares as a means of monitoring the identity of such companies by, for example, requiring custody by:

⁸ **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 PEP, either socially or professionally.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- a. The financial institution, or its subsidiary, regulated affiliate, parent or holding company;
- b. A recognized regulated financial institution in a jurisdiction with equivalent AML/CFT standards; and
- c. Requiring the prior approval before shares can be exchanged.

6.5 No Simplified Due Diligence for Higher Risk Scenarios

Simplified customer due diligence should be unacceptable for specific higher-risk scenarios. Higher-risk scenarios may include, but are not limited to the following:

- A customer is not physically present for identification purposes; or
- The nature of the situation is such, or a risk assessment reveals, that a higher risk of money laundering and the financing of terrorism are likely.

6.6 Higher Risk Countries

Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and consequently may pose a higher potential risk to financial institutions. Conducting business relationships with customers who are either citizens of or domiciled in such countries may expose the financial institution to reputational risk. Financial institutions are encouraged to consult publicly available information to ensure that they are aware of countries/territories which may pose a higher risk.

6.7 Retrospective Due Diligence

Where the identity information held on existing customers does not comply with the requirements of this guideline, financial institutions are required to develop a risk-based programme for ensuring compliance. Financial institutions must:

- i. Record their non-compliant business relationships, noting what information or documentation is missing;
- ii. Establish a framework for effecting retrospective due diligence, including the setting of deadlines for the completion of each risk category. The timing of retrofitting can be linked to the occurrence of a significant transaction, a material change in the way that an account is operating, or doubts about previously obtained customer due diligence data; and



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- iii. Establish policies for coping with an inability to obtain information and documentation, including terminating the relationship and making a suspicious report.

Where a financial institution deems on the basis of risk and materiality, that it is not practical to retrofit a customer (e.g. the settlor has died; the account is inactive or dormant), exemption of such accounts must be approved by the compliance officer and senior management, ratified by the board and documented on the individual's file.

6.8 Reduced Customer Due Diligence

As discussed in Section 5.1, the financial institution's policy document should clearly define the risk categories/approach that is adopted and associated due diligence, monitoring and other requirements. A financial institution may apply reduced due diligence to a customer provided that it satisfies itself that the customer is of such a risk level that qualifies for this treatment. The financial institution will of necessity have to identify the customer as part of the process of confirming that the reduced due diligence apply but, will not be required to re-verify the identity of the customer or beneficial owner or obtain information on the purpose or intended nature of the business relationship. Financial institutions should note their obligations with regard to ongoing monitoring of the business relationship. The reduced due diligence should be commensurate with the lower risk factors. Financial institutions have to conduct and document appropriate testing to satisfy themselves that the customer or counterparty qualifies for the reduced due diligence. Examples of possible measures are:

- Verifying the identity of the customer (e.g. if account transactions rise above a defined monetary threshold, or if it is largely impractical to do so);
- Reducing the frequency of customer identification updates;
- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold;
- Not collecting specific information or conducting specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Such circumstances which may warrant reduced due diligence measures are set out below:

- i) Where an application to conduct business is made by:
 - a. An entity regulated by the Central Bank of Barbados under the International Financial Services Act or the Financial Institutions Act;



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- b. An entity regulated by the Financial Services Commission;
 - c. The Government of Barbados; or
 - d. A statutory body of the Barbados Government or that of a jurisdiction that is not included on the FATF's high risk and non-cooperative jurisdictions or the UN Security Council's sanctions list.
 - c. An entity supervised and regulated by a regulated body or listed on a stock exchange in a jurisdiction not included on the FATF's high risk and non-cooperative jurisdictions list or the UN Security Council's sanctions list.
- ii) Where there is a transaction or series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity.
- iii) Where an existing customer opens a new account unless the condition described at Section 6.7, sub-item (ii) holds. However, if the source of funds/wealth originates from an external source, or from a country where, for example, it is believed or known that there is a high level of drug trafficking or corruption, reduced due diligence must not apply.
- iv) Where a financial institution acquires the business of another financial institution, whether in Barbados or elsewhere, and it is satisfied that the due diligence standards of the acquired institution are at least equivalent to that set in this guideline, it need not re-verify the customers.

Notwithstanding the foregoing, financial institutions must not apply reduced due diligence where there is a suspicion of money laundering or terrorist financing. Further, if the financial institution is not satisfied that equivalent standards have been followed or the customer records are not consistent with the requirements of this guideline, the financial institution must seek to identify and verify the identity of customers who do not have existing relationships with the financial institution along the lines set out in Section 6.7.

7.0 UNUSUAL & SUSPICIOUS TRANSACTIONS

Suspicious transactions are financial transactions that give rise to reasonable grounds to suspect that they are related to the commission of a money laundering or terrorism offence. These transactions may be complex, unusual or large or may represent an unusual pattern. This includes significant transactions relative to the relationship, transactions that exceed prescribed limits or a very high account turnover that is inconsistent with the expected pattern of transactions. In some instances, the origin of the transaction may give rise to



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

suspicion. For examples of “Red Flags” see **Appendix 7**.

A pre-requisite to identifying unusual and suspicious activity is the profiling of customers and determination of consistent transaction limits. Unusual transactions are not necessarily suspicious, but they should give rise to further enquiry and analysis. In this regard, financial institutions must examine, to the extent possible, the background and purpose of transactions that appear to have no apparent economic or visible lawful purpose, irrespective of where they originate.

Financial institutions must develop procedures to assist in the identification of unusual or suspicious activity in all types of business transactions, products and services.

A financial institution must:

- i. Develop effective manual and/or automated systems to enable staff to monitor, on a solo, consolidated and group-wide basis, transactions undertaken throughout the course of the business relationship and identify activity that is inconsistent with the financial institution’s knowledge of the customer, their business and risk profile; and
- ii. Determine customer specific limits based on an analysis of the risk profile of customers, the volume of transactions and the account turnover. When applied, this may give rise to multiple limits and/or aggregate limits on a consolidated basis.

Financial institutions must not grant blanket exemptions and must:

- i. Clearly document their policy for the granting of such exemptions including the qualifying criteria for exemption, officers responsible for preparing and authorizing exemptions, the basis for establishing threshold limits, review of exempt customers and procedures for processing transactions.
- ii. Maintain authorised exempt lists showing threshold limits established for each qualifying customer.

For the purposes of this guideline, and consistent with Section 2 of the MLFTA, a transaction includes an attempted or aborted transaction.

7.1 Internal Reporting Procedures

To facilitate the detection of suspicious transactions, a financial institution must:



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- i. Require customers to declare the source and/or purpose of funds for business transactions in excess of threshold limits, or such lower amount as the financial institution determines, to reasonably ascertain that funds are not the proceeds of criminal activity. **Appendix 8** 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 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 FIU (See Section 7.2);
- iv. Require its staff to document in writing their suspicion about a transaction; and
- v. Require documentation of internal enquiries.

7.2 External Reporting

Financial institutions 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 financial institution 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.

In addition, pursuant to the United Nations Resolutions on terrorist financing, financial institutions must freeze any funds or other assets held for individuals or organisations listed on the UN list of persons connected to terrorism, and submit a report to the FIU. This list may be accessed at www.un.org⁹.

Where a suspicious report has been filed with the FIU, and further unusual or suspicious activity pertaining to the same customer or account arises, financial institutions must file additional reports with the FIU.

⁹ <http://www.un.org/Docs/sc/committees/1267/1267ListEnglish.htm>



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Licensed financial institutions, their directors, officers, employees and agents are protected under the MLFTA from any action, suit or proceedings for breach of any restriction on disclosure of information, if they report suspicious activity in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. See sections 48(5) and 48(6) of the MLFTA. It is against the law for employees, directors, officers or agents of a financial institution to disclose that a suspicious transaction report or related information on a specific transaction has been reported to the FIU.

Reports must be in the format determined by the FIU (See **Appendix 9**). However, where a matter is considered urgent, an initial report may be made by contacting the FIU by telephone or e-mail.

Where a person is a client of both the financial institution and another group member, and a suspicious report is prepared by the latter, the Barbados FIU must be notified.

8.0 COMPLIANCE AND AUDIT

Financial institutions must designate a suitably qualified person at the management level with the appropriate level of authority, seniority and independence as Compliance Officer or indicate an individual whose function includes AML compliance. The Compliance Officer must be independent of the receipt, transfer or payment of funds, or management of customer assets, and should have timely and uninhibited access to customer identification, transaction records and other relevant information. The powers and reporting structure of the officer should be conducive to the effective and independent exercise of duties.

The Compliance Officer must:

- i. Undertake responsibility for developing compliance policies;
- ii. Develop a programme to communicate policies and procedures within the entity;
- iii. Monitor compliance with the financial institution's internal AML programme;
- iv. Receive internal reports and consider all such reports;
- v. Issue, in his/her own discretion, external reports to the FIU as soon as practicable after determining that a transaction warrants reporting;
- vi. Monitor the accounts of persons for whom a suspicious report has been made;
- vii. Establish and maintain on-going awareness and training programmes for staff at all levels;



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- viii. Establish standards for the frequency and means of training;
- ix. Report at least annually to the board of directors (or relevant oversight body in the case of branch operations) on the operations and effectiveness of the systems and controls to combat money laundering and the financing of terrorism;
- x. Review compliance policies and procedures to reflect changes in legislation or international developments;
- xi. Participate in the approval process for high-risk business lines and new products, including those involving new technologies; and
- xii. Be available to discuss with the FSC or the FIU matters pertaining to the AML/CFT function.

The internal audit department must carry out reviews to evaluate how effectively compliance policies are being implemented. Such reviews must be carried out on a frequency consistent with the financial institution's size and risk profile. The review process must identify and note weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions.

The FSC recognises, however, that the designation of a Compliance Officer or the creation of an internal audit department may create difficulties for some small financial institutions. Where this is not possible, a financial institution may, subject to the FSC's agreement, outsource the operational aspects of the compliance or internal audit function to a person or firm that is not involved in the auditing or accounting functions of the financial institution.

Notwithstanding, the responsibility for compliance with the MLFTA and the guideline remains that of the financial institution and the requirements of this section will extend to the agent. A financial institution must always be ready to respond to the FSC and the FIU on AML/CFT issues.

9.0 RECORD-KEEPING

To demonstrate compliance with the MLFTA and to facilitate investigations undertaken by the FIU, financial institutions must establish a document retention policy that provides for the maintenance of a broad spectrum of records, including those related to customer identification, business transactions, internal and external reporting and training.

Financial institutions must maintain these records for a minimum of **five years**, in accordance with Section 18 (2) (a) of the MLFTA, after the termination of the business transaction, or the business relationship, whichever is applicable.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

However, it may be necessary for financial institutions to retain records, until such time as advised by the FIU or High Court, for a period exceeding the date of termination of the last business transaction where:

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

Financial institutions must ensure that records held by an affiliate outside Barbados at a minimum, comply with the requirements of Barbados law and this guideline.

Financial institutions must retain records in a format, including electronic, scanned or microfilm, that would facilitate reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity and to enable financial institutions to comply swiftly with information requests from the FIU. This applies whether or not records are stored off the premises of the financial institution.

When a financial institution merges with or takes over another entity, it must ensure that the records described above can be readily retrieved. Where the records are kept in a contractual relationship by an entity other than a financial institution, the financial institution is responsible for retrieving those records before the end of the contractual arrangement.

The nature of records that must be retained is set out at Section 2 of the MLFTA, which defines a business arrangement, business transaction, and business transaction record.

9.1 Internal and External Records

In accordance with section 18(2) of the MLFTA, financial institutions must maintain records related to unusual and suspicious transaction reports. These must include:

- i. All reports made by staff to the Compliance Officer;
- ii. The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made;
- iii. Consideration of those reports and of any action taken; and
- iv. Reports by the Compliance Officer to senior management and board of directors.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

9.2 Training Records

In order to provide evidence of compliance with Section 21 of the MLFTA, at a minimum, a financial institution must maintain the following information:

- Details and contents of the training programme provided to staff members;
- Names of staff receiving the training;
- Dates that training sessions were held;
- Test results carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An on-going training plan.

10.0 TRAINING AND AWARENESS

An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analysing potential illicit transactions. Financial institutions must, therefore, establish ongoing employee training programmes. Training must be targeted at all employees but added emphasis must be placed on the training of the Compliance Officer and the compliance and audit staff because of their critical role in sensitising the broader staff complement to AML/CFT issues and ensuring compliance with policy and procedures. Additionally front line staff should be targeted so as to enable them to respond appropriately when interacting with the public.

Financial institutions, therefore, must:

- i. Develop an appropriately tailored training and awareness programme consistent with their size, resources and type of operation to enable their employees to be aware of the risks associated with money laundering and terrorist financing, to understand how the institution might be used for such activities, to recognise and handle potential money laundering or terrorist financing transactions and to be aware of new techniques and trends in money laundering and terrorist financing;
- ii. Clearly explain to staff the laws, the penalties for non-compliance, their obligations and the requirements concerning customer due diligence and suspicious transaction reporting;
- iii. Formally document, as part of their anti-money laundering policy document, their



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- approach to training, including the frequency, delivery channels and content;
- iv. Ensure that all staff members are aware of the identity and responsibilities of the Compliance Officer and/or the Reporting Officer to whom they must report unusual or suspicious transactions;
 - v. Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required for:
 - a. New hire orientation;
 - b. Operations staff;
 - c. Supervisors;
 - d. Board and senior management; and
 - e. Audit and compliance staff.
 - vi. Obtain an acknowledgement from each staff member on the training received; and
 - vii. Provide all staff with reference manuals/materials that outline their responsibilities and the institution's policies. These should complement rather than replace formal training programmes.

10.1 Content and Scope of the Training Programme

A financial institution's overall training programmes must cover topics pertinent to its operations and must be informed by developments in international AML/CFT standards. Training should be general as well as specific to the area in which the trainees operate. As staff members move between jobs, their training needs for AML/CFT may change. Training programmes must, inter alia, incorporate references to:

- i. Relevant money laundering and terrorism financing laws and regulations;
- ii. Definitions and examples of laundering and terrorist financing schemes;
- iii. How the institution can be used by launderers or terrorists;
- iv. The importance of adhering to customer due diligence policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;
- v. Effective ways of determining whether clients are PEPs and to understand, assess and handle the potential associated risks;



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- vi. The procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;
- vii. The completion of unusual and suspicious transaction reports;
- viii. Treatment of incomplete or declined transactions; and
- ix. The procedures to follow when working with law enforcement or the FIU on an investigation.

11.0 PRE-EMPLOYMENT BACKGROUND SCREENING

The ability to implement an effective AML/CFT programme depends in part on the quality and integrity of staff. Financial institutions must, therefore, undertake due diligence on prospective staff members. The senior management of a financial institution must:

- i. Verify the applicant's identity;
- ii. Develop a risk-focussed approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual staff member may warrant additional background screening, which must include verification of references, experience, education and professional qualifications.
- iii. Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of departmental staff over a period of time. Internal policies and procedures must be in place (e.g. codes for conduct, ethics, conflicts of interest) for assessing staff; and
- iv. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

12.0 SECTOR SPECIFIC GUIDANCE

This section is intended to deal with specialised areas of relevant financial business which require more explanation and raise more complex issues than are dealt with in the general body of this guideline. This section must be read in conjunction with the other sections of this guideline.

For the purposes of this guideline relevant insurance business (RIB) means any entity, including any exempt insurance company or qualified insurance company which is licensed by the FSC to conduct insurance business in or from Barbados, and is engaged in the following types of insurance business;

- I. A permanent life insurance policy other than a group life insurance policy
- II. Any annuity contract, other than a group annuity contract and
- III. Any other individual life insurance product with features of cash value or investment
- IV. Any general insurance business
- V. Any intermediary selling or placing insurance business with a financial institution

12.1 Insurance

Life insurance and long term insurance products are the predominant classes of insurance used by money launderers; however some money-laundering activities could be employed through the use of non-life insurance as well. There are several types of life insurance products including term, whole life, and combinations of these types. There are also single or regular premium unit-linked life assurance policies in which units are linked to the value of the underlying investments. Unit-linked policies are the types which are more subject to abuse. Typically, in the context of AML guidance, and measured on a risk basis. Life and non-life activities should be separated, and where policies are hybrid in nature, for example, life insurance and investment, the funds should be appropriately segregated.

Where a transaction involves an insurer and an intermediary, each needs to separately consider its own position and to ensure that its own obligations under this guideline and the MLFTA are duly discharged. In this regard there will be a necessity for KYC information sharing between intermediaries, as the first point of contact or outset of the relationship, and the insurer as the entity paying claims. An information share system should be put in place between insurer and intermediary to allow both entities to satisfy the requirements under the MLFTA. The KYC information shared should be used solely for the purpose of completing the KYC requirements unless otherwise stated in a formal agreement signed between the insurer and the intermediary.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

As part of their due diligence process RIBs should:

- i. Establish procedures for obtaining identification information on new customers so as to be satisfied that a prospective customer is who he claims to be;
- ii. Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset of a business relationship; and
- iii. Except in instances outlined in section 6.8 of the guideline, ensure that they have adequate procedures:
 - a. To retain all post sale records associated with the maintenance of the contract, up to and including the point of maturity; and
 - b. Provide details of maturity processing and claim settlement including completed "discharge of obligation".

For the purposes of this guideline, the RIB should seek to identify the customer and all those who exercise control over the policy holder. A customer includes:

- i. A person or entity that maintains a policy/contract with the RIB;
- ii. A person or entity on whose behalf a policy/contract is maintained i.e. beneficial owner;
- iii. The beneficiaries of business transactions conducted by professional intermediaries such as lawyers, accountants, notaries, business introducers or any other professional service providers;
- iv. A person or entity entering into an arrangement with an intermediary through who a policy/contract is placed with a third party entity or insurer; or
- v. Any person or entity connected with a financial institution that can pose a significant risk to the RIB, including persons establishing business arrangements, purporting to act on behalf of a customer or conducting business.

In effecting the due diligence process, RIBs should:

- i. Whenever possible, require prospective customers to be interviewed in person. In cases of an exempt insurance company or a qualifying insurance company where the ultimate transaction is outside of Barbados, RIBs should ensure that appropriate customer due diligence is conducted at source. Exceptions to this are outlined in Sections 6.8;
- ii. In verifying customer identity, use independent official or other reliable source documents, data or information to verify the identity of the beneficial owner prior to opening the account or establishing the business relationship.
- iii. 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 open an



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

account. Examples of documentation for different types of customers are set out in Sections 6.1 to 6.5.

Generally, RIBs should not accept funds from prospective customers unless the necessary verification has been completed. In exceptional circumstances, where it would be essential not to interrupt the normal conduct of business (e.g. non face-to-face business and securities transactions), verification may be completed after establishment of the business relationship. Should this be determined to be an acceptable risk, RIBs should adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. If the requirements are not met, and it is determined that the circumstances give rise to suspicion, then the RIB should make a report to the FIU.

Procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being conducted outside of expected norms for that type of relationship. Where there is a suspicion that a transaction relates to money laundering or the financing of terrorism, RIBs should be cognizant of tipping off a customer when conducting due diligence. The RIB should make a business decision whether to open the account or execute the transaction as the case may be, but a suspicious report should be submitted to the FIU.

12.2 Mutual Funds and Mutual Fund Administrators

In this section:

a "Mutual Fund" or "Fund" is as defined in accordance to the Mutual Funds Act 2002 CAP 320B, (*"the MFA"*) as:

- (a) a registered unit trust;
- (b) a company;
- (c) a partnership; or
- (d) a society,

that has been granted a licence under this Act for the purpose of carrying on mutual fund business in or from Barbados in compliance with this Act, but does not include:

- (i) a person licensed under



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- 1.1. Part II of the *Financial Institutions Act*, other than a finance company;
- 1.2. the *Insurance Act*; and
- 1.3. the *Exempt Insurance Act*;

(ii) a friendly society within the meaning of the *Friendly Societies Act*;

(iii) a society, financial institution or association within the meaning of the *Co-operative Societies Act*;

(iv) any company or partnership, whether Barbadian or foreign, that is primarily engaged in any industrial, commercial or charitable enterprise and may include a unit trust.

A "Licensed Mutual Fund Administrator" or "An Administrator" means the holder of a general administration licence or a restricted administration licence granted under the Mutual Funds Act. That is: a person managing or administering a Mutual Fund (including controlling all or substantially all of its assets); a person providing the principal office of a mutual fund in Barbados or providing an operator to the mutual fund as defined in section 2 of the Mutual Funds Act CAP 320B.

A "Promoter" is as defined in section 2 of the Mutual Funds Act CAP 320B; namely, any person who causes the preparation or distribution of an offering document in respect of a Mutual Fund or proposed Fund. This does not include a professional adviser acting for or on behalf of the aforementioned persons.

12.2.1 Timing of Verification

The MLFTA provide that there should be procedures in place requiring, as soon as reasonably practicable after contact is first made with an applicant for business, either satisfactory evidence of the applicants identity or that steps are taken which will produce satisfactory evidence of identity. The time span in which satisfactory evidence has to be obtained depends on the particular circumstances and the practicalities of obtaining evidence before commitments are entered into between parties and before money passes.

In the Fund context, situations may arise in which satisfactory identification procedures have not been completed prior to the receipt of subscription funds or redemption settlement requests. Whether or not it is appropriate to transfer funds to a brokerage or similar account in the name of the Fund may depend on the nature of the investment. Mutual funds and administrators should ensure that they have implemented a tightly-controlled procedural framework to ensure that shares/units/interests are not applied to investors and that redemption proceeds are not settled without senior management approval, the basis for such approval to be recorded and such records retained.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

If, after having conducted a risk assessment in accordance with section 6 of the guideline, verification procedures or identification of an investor have not been completed prior to the date on which redemption is due to take place, the mutual fund should use the opportunity of redemption to seek satisfactory evidence of identity. It is industry best practice that, save in exceptional circumstances, payment of the redemption proceeds should be made only to the investor and not to a third party. In all circumstances the requisite level of due diligence on a risk basis should have been employed

12.2.2 Client verification – Assumed Business

Where a successor firm is acquiring administration of an existing mutual fund, the successor must ensure that the necessary due diligence has been performed prior to performing the administration. It may be possible to rely upon the evidence of identity obtained by a predecessor administrator provided that the original files, or certified copies of the original files, are transferred to the successor administrator and the successor firm has assessed the quality of the evidence on investor identity. Where insufficient evidence exists, it may be appropriate to supplement with additional evidence to meet the standards required by this guideline.

12.2.3 Fund Compliance Procedures

Regulated financial institutions must have internal reporting procedures in place to (1) identify and report suspicious activity, (2) monitor and ensure internal compliance with laws relating to money laundering, and (3) test the AML/CFT system consistent with the MLFTA and this guideline. Both mutual funds and their administrators have separate obligations to maintain and implement procedures in respect of their relevant financial business. Although ultimate responsibility for maintaining and implementing satisfactory procedures remains with the financial institution, the obligations may be met by delegating or outsourcing those functions. A fund can meet its obligations in relation to the procedures in a number of ways:

- i. It can implement procedures directly;
- ii. Where a fund has no staff in Barbados and the administration of subscriptions and redemptions is conducted by a person subject to the anti-money laundering regime of Barbados, in a jurisdiction not included in the FATF's list of high risk and non-cooperative jurisdictions, or on the UN Security Council's sanctions list, the fund will be regarded by the FSC as being compliant with the guideline if the fund's reliance on such a person is acknowledged in an appropriate agreement (e.g., an administration or registrar and transfer agency agreement), and if the person administering subscriptions and redemptions does so in compliance with the applicable procedures of such jurisdiction;



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- iii. Where a fund has delegated any of the procedures to a person subject to the anti-money laundering regime of the Barbados or an approved jurisdiction, consistent with the requirements of the guideline, where applicable, the fund will be regarded by the FSC as being compliant with the guideline; and
- iv. A fund may also delegate any or all of its obligations with respect to the maintenance of Procedures to a suitable third party or parties, whether within or outside Barbados, provided that such appointment is consistent with the requirements of sections 6-11 of the guideline, where applicable;
- v. A fund administrator may delegate any of the requirements of this guideline to a regulated person in Barbados or a person in a jurisdiction not included in FATF's list of high risk and non-cooperative jurisdictions that is subject to the AML/CFT regime of that country, consistent with the requirements of the guideline, where applicable. The fund administrator will be regarded by the FSC as being compliant with the guideline with respect to the procedures if the delegate complies with the procedures of such jurisdiction; and
- vi. A fund administrator may also delegate any or all of its obligations with respect to the maintenance of the requirements of this guideline to a suitable third party or parties, whether within or outside the Barbados, provided that such appointment is consistent with the requirements of sections 6-11 of the guideline, where applicable.

Notwithstanding the above, the operators of a fund or the fund administrator should document, either as a board resolution or otherwise, the manner in which the entity has met its obligation to maintain procedures outlined in this guideline.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

12.3 Market Actors: Securities and Investment Business

Introduction

Market actors are less likely to be at risk during the initial placement stage of money laundering because cash settlement of investment transactions is relatively rare. Instead, in the securities and investment business, it is more likely that market actors will come into contact with the layering and integration stages of a money laundering operation than the placement of cash. Often the money launderers' intention will be simply to carry out transactions for their own purposes, and to complicate the audit trail in the event of an investigation at a later stage.

Layering and integration of laundered money tend to occur in the securities and investment businesses because the liquidity of many investment products attracts sophisticated money launderers, as it allows them the opportunity to move funds quickly and easily from one product to another, mixing lawful and illicit proceeds and integrating them into the legitimate economy. Investment businesses are also able to transfer monies across borders quickly and efficiently. Complex and sophisticated new investment products that are constantly being introduced, and the lack of order in emerging markets, offer considerable potential to the money launderer.

Procedures and records maintained by investment businesses constitute an important audit trail and play an important part in combating money laundering.

Table 1: Identification of Customer/Counterparty

The applicant for business may be one of the following:

Where the Market Actor	Applicant for Business is
acts as agent in buying, selling, managing, subscribing for or underwriting securities	the principal
acts as principal or makes arrangements in buying, selling, managing, subscribing for or underwriting securities	the counterparties
advises an investor or potential investor on the merits for buying, selling, managing subscribing for or underwriting securities	the investor or potential investor



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

12.3.1 Client Verification

Client verification information should be obtained prior to opening account or establishing business relationship. If it is not forthcoming at the outset or within a reasonable time, the relationship should be re-evaluated and transactions should not proceed. For exceptions, refer to section 6.8 of this guideline.

If the market actor acquires the clients/accounts of another market actor, if the money laundering procedures previously undertaken have not been in accordance with Barbados requirements, or the procedures cannot be checked by the market actor acquiring the new customer, or the customer records are not available to the acquiring market actor, then verification of identity procedures will need to be undertaken for all transferred customers as soon as is practicable.

Market actors should use their judgment in determining whether or not in the context of the intended business relationship they should place reliance on the due diligence procedures of intermediaries. In cases in which reliance is placed on the intermediary, senior management must make a judgement as to whether or not it would be prudent to obtain appropriate evidence of client verification either by provision by the introducer of primary documentation relating to confirm identity, or by written confirmation from the introducer that it has satisfied itself as to the *bona fides* and integrity of the client. This is further explained in section 6.4.4 of this guideline "Introduced Business,".

Table 2: Information Requirements

Applicant for Business	Information which should be obtained
Where the principal, counterparty(ies), or investor or potential investor is a person	Sufficient information to anticipate normal business activity, including type of products required and general level of likely activity and investment goals.
Where the principal, counterparty(ies), or investor or potential investor is a company, or otherwise	<p>Sufficient information to anticipate normal business activity, including type of products required and general level of likely activity and investment goals; and</p> <p>Sufficient information regarding intra-group relationships, if any; clients; service providers; and trading partners to establish a trading profile which can be monitored against transactions.</p>



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

12.3.2 Enhanced Due Diligence, Warning Signs and Suspicious Transactions

The aim of the money launderer is to introduce as many layers as possible. This means that the money may pass through a number of sources and through a number of different persons or entities. Of note, long-standing and apparently legitimate customer accounts may be used to launder money or finance terrorist activity innocently, as a favour, or due to the exercise of undue pressure. Settlement also poses an area of risk for market dealers, payment through a third-party cheque or a money transfer where there is a variation between the account holder, the signatory and the prospective investor should give rise to additional enquiries. One should note that cash settlement through a third party is not in itself suspicious, but poses an area of vulnerability. Enhanced due diligence may also be applied in situations where the market actor is particularly exposed to reputational risk. Section 6.4 of the guideline provides information on procedures in dealing with situations that require enhanced due diligence.

Appendix 7 of the Guidelines contains examples of “red flags” for which market actors must be alert. The following list contains additional “red flags” which may indicate a money laundering scheme. As stated at Appendix 7, the presence of any of the following behaviours does not necessarily indicate an inappropriate or illegal act, but the market actors should be on enquiry and be satisfied with any explanation, especially as more and more of the activities listed below are present.

- i. Clients who are unknown to the market actors and verification of identity / incorporation proves difficult;
- ii. Clients who wish to deal on a large scale but are completely unknown to the market actor;
- iii. Clients who wish to invest or settle using cash;
- iv. Clients who use a cheque that has been drawn on an account other than their own;
- v. Clients who change the settlement details at the last moment;
- vi. Clients who insist on entering into financial commitments that appear to be considerably beyond their means;
- vii. Clients who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
- viii. Clients who have no obvious reason for using the services of the market actor (e.g. clients with distant addresses who could find the same service nearer their home base);
- ix. Clients whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere;



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- x. Clients who refuse to explain why they wish to make an investment that has no obvious purpose;
- xi. Clients who are introduced by an overseas agent based in a country noted for drug production or distribution or a client introduced by an overseas branch, affiliate or other service provider based in a jurisdiction that is included in FATF's list of high risk and non-co-operative jurisdictions;
- xii. Clients who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from a jurisdiction included in the FATF's list of high risk and non-cooperative jurisdictions;
- xiii. Clients who transfer funds or shares to accounts in a jurisdiction that is included in the FATF's list of high risk and non-cooperative jurisdictions;
- xiv. Clients who make back to back deposit/loan transactions with subsidiaries or affiliates of overseas financial services businesses;
- xv. Clients who want to transfer funds overseas or make payment in foreign currency which appear to have no commercial objective;
- xvi. Clients who indulge in much activity with little or no profit over a number of jurisdictions;
- xvii. Clients who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
- xviii. Clients who purchase low grade securities in an overseas jurisdiction, sell locally and then purchase high grade securities with the proceeds;
- xix. Clients who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
- xx. Clients who wish to maintain a number of trustee or clients' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
- xxi. Any transaction involving an undisclosed party;
- xxii. Transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
- xxiii. There is significant variation in the pattern of investment with reasonable or acceptable explanation.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Market actors also need to be aware that its employees could be targeted by money launderers and therefore should be aware of:

- i. Changes in employee characteristics (e.g. lavish life styles or avoiding taking holidays); and
- ii. Changes in employee or agent performance, (e.g. a dealer has remarkable or unexpected increase in performance).



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

APPENDICES

Appendix 1

Coverage of Activities of Financial Institutions

Although MLFTA applies to all persons and businesses, additional administrative requirements are placed on financial institutions.

The activities of financial institutions are defined in the **First Schedule** of the MLFTA as follows:

1. Acceptance of deposits and other repayable funds from the public, including private banking.
2. Lending, including consumer credit, mortgage credit, factoring (with or without recourse), and financing of commercial transactions, including forfeiting.
3. Financial leasing other than with respect to arrangements relating to consumer products.
4. Money or value transmission services.
5. Issuing and managing means of payment, including credit and debit cards, travellers' cheques, money orders and bankers' drafts, and electronic money.
6. Issuing financial guarantees and commitments.
7. Trading in
 - (a) money market instruments, including cheques, bills, certificates of deposit and derivatives;
 - (b) foreign exchange;
 - (c) exchange, interest rate and index instruments; and
 - (d) transferable securities.
8. Commodity futures trading.
9. Participation in securities issues and the provision of financial services related to such issues.
10. Individual and collective portfolio management.
11. Safekeeping and administration of cash or liquid securities on behalf of other persons.
12. Investing and administering or managing funds or money on behalf of other persons.
13. Underwriting and placement of life insurance and other investment-related insurance, including insurance intermediation by agent and brokers.
14. Money and currency changing.
15. Any other service of a financial nature.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 2

Additional References

Name of Organisation	Website Address / Link
Basel Committee on Banking Supervision	http://www.bis.org/bcbs/
Caribbean Financial Action Task Force (CFATF)	www.cfatf-gafic.org/
Commonwealth Secretariat	http://www.thecommonwealth.org
Egmont Group for Financial Intelligence Units	http://www.egmontgroup.org
Financial Action Task Force (FATF)	http://www.fatf-gafi.org
Financial Stability Forum	http://www.fsforum.org
International Association of Insurance Supervisors	http://www.iaisweb.org
International Monetary Fund	www.imf.org
International Organisation of Securities Commission	http://www.iosco.org
Interpol (Interpol's involvement in the fight against international terrorism)	http://www.interpol.com/public/terrorism/default.asp
Organisation of American States – CICAD	http://www.cicad.oas.org
The Financial Crime Enforcement Network (FINCEN)	http://www.fincen.gov/af_main.html
The World Bank	http://www.worldbank.org
United Nations	http://www.un.org
United Nations – International Money Laundering Information Network	http://www.imolin.org
United Nations – Security Council Resolutions	http://www.un.org/en/sc/documents/resolutions/
United Nations Office on Drugs and Crime	http://unodc.org
US Department of the Treasury, Comptroller of the Currency Administrator of National Banks (Money Laundering: A Banker's Guide to Avoiding Problems)	http://www.occ.treas.gov/topics/bank-operations/financial-crime/money-laundering/money-laundering-2002.pdf
Wolfsberg Group	http://www.wolfsberg-principles.com/index.html



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 3(a)

Summary of Money Laundering and Terrorism Sanctions Offences

Area	Description of Offence	Description of Fine	Section of Legislation
Reporting Obligations	Failure of financial institution to make a report on a suspicious transaction to the FIU.	\$100,000 on directors jointly and severally	Section 22 (2) of the MLFTA
	Failure of a financial institution to maintain business transactions records.	\$100,000 on directors jointly and severally	Section 18 (4) of the 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) of the 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) of the MLFTA
Internal Policies, procedures, controls; Internal employee training and awareness programs	Failure by a financial institution 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
Information Gathering and Investigation	Failure by a financial institution 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 FSC.	The licence of the financial institution may be suspended.	Section 31(4) of the MLFTA
Interference in the	The obstruction, hindrance,	\$50,000 or imprisonment of 2	Section 42



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Area	Description of Offence	Description of Fine	Section of Legislation
Line of Duty	molestation or assault to any member of the Authority, constable or other person in performing duties under the Act.	years or both	of the 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 FSC to cease and desist.	Section 33 of the MLFTA
Money Laundering Offences	Engagement of 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) of the MLFTA Section 35 & 46(1) of the MLFTA
	Providing assistance to engage in money laundering.	Summary conviction - \$150,000 or 3 years imprisonment or both. Conviction on indictment - \$1,500,000 or 15 years imprisonment or both	Section 6(2) of the MLFTA
	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 of the 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) of the 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) of the MLFTA.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

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 ¹⁰ 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

¹⁰ 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.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 3(b)

Summary of Administrative Sanctions

Description of Offence	Sanctions Enforceable by the Anti-Money Laundering Authority or Financial Services Commission	Section of Legislation
<p>Failure to meet fitness and propriety standards</p> <p>Failure to comply with or contravene a guideline issued in accordance with section 26 of the MLFTA or section 53 (1 e) of the FSC Act</p> <p>Failure to comply with a directive given in accordance with section 33</p>	<p>Any of the following:</p> <p>Issue a warning or reprimand to the financial institution,</p> <p>Give such directives as deemed appropriate,</p> <p>Impose on the financial institution, in accordance with section 36, a pecuniary penalty*, or</p> <p>Recommend, in accordance with section 35:</p> <ul style="list-style-type: none"> (i) Suspension of any or all of the activities that the financial institution may otherwise conduct pursuant to the licence of the financial institution; or (ii) Suspension or revocation of the licence of the financial institution. 	<p>Section 34 of the MLFTA</p>
<p>The financial institution is otherwise contravening the Act.</p>	<p>*Pecuniary Penalties Enforceable by the Anti-Money Laundering Authority or FSC:</p> <p>Where the FSC is satisfied as to any of the circumstances referred to in section 34(1) in respect of a financial institution, the FSC may, by written notice, impose on the financial institution, a pecuniary penalty not exceeding \$5,000.</p> <p>Where by this Act or guideline made or directive given under this Act a financial institution is required, by a specified time, to take certain measure or action or cease a particular activity, behaviour or practice and the FSC is satisfied that the financial institution has failed to do so, the FSC may impose on the financial institution, in addition to the penalty specified in subsection (1), an additional penalty of \$500 for every day or part of a day that the financial institution failed to take the measure or action or cease the particular activity, behaviour or practice.</p>	<p>Section 36 of the MLFTA</p>



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 4

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.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013**

Appendix 5

Approved Persons for Certification of Customer Information

In keeping with Section 7.4.3 on non face-to-face customers, financial institutions must 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



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 6

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:



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 6 (cont'd)

Confirmation of Customer Verification of Identity

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:



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 7

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 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.

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

If the Client:

- Starts conducting frequent cash transactions in large amounts when this has not been a normal activity in the past.
- Frequently exchanges small bills for large ones.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

- Deposits 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 makes cash transactions that are just under the reporting threshold amount in a 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.

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.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

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 transfer 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



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

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 Authority 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.



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

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 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 and/or invitations from certain clients, with no clear or reasonable 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).



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 8

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)



AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Appendix 9

Suspicious/Unusual Transaction Report

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 possible AFTER the dealing, and a copy forwarded to:

THE DIRECTOR, FINANCIAL INTELLIGENCE UNIT
ANTI-MONEY LAUNDERING AUTHORITY

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

3. If yes, original Report's date: ____/____/____
D M Y

4. Reporting date: ____/____/____
D M Y

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



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

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

PART B – Identity of Customer 1

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
Passport
Driver's Licence
Other: _____ 9. _____
ID No. (1)

10. _____
Place of Issue

11. Identifier #2 ID Card
Passport
Driver's Licence
Other: _____ 12. _____
ID No. (2)

13. _____
Place of Issue

14. _____ 15. _____
Occupation Employer

16. _____



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

Tel # (Include area code) (H)	Tel # (Include area code) (W)	Tel # (Include area code) (C)
-------------------------------	-------------------------------	-------------------------------

17. _____
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

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 Licence Other: _____	9. _____ ID No. (1)
		10. _____ Place of Issue

11. Identifier #2	ID Card Passport Driver's Licence Other: _____	12. _____ ID No. (2)
		13. _____ Place of Issue

14. _____

15. _____



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

-
16. _____
Occupation Employer
Tel # (Include area code) (H) Tel # (Include area code) (W) Tel # (Include area code) (C)
17. _____
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 more than one customer at the counter.

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. _____ 2. _____ 3. _____
Surname Given Name Middle Name(s)
4. _____ 5. _____
Alternative Entity's Name 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 Licence Other: _____
9. _____ 10. _____
ID No. (1) Place of Issue



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

11. _____
Occupation/Type of Business
12. _____
Employer
13. _____
Tel # (Include area code) (H) Tel # (Include area code) (W) Tel # (Include area code) (C)
14. _____
Email Address #1 Email Address #2
15. _____
Account Number(s)
16. _____
State if account is 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 Jewellery
Purchase of precious metals/stones
Purchase of gold
Securities

Conducted Currency Exchange
Inter-account transfer
Outgoing electronic funds transfer
Purchase of diamonds
Purchase of money order
Purchase of traveller's cheques
Real Estate Purchase
Other: _____

2. Date(s) of transaction(s): ____/____/____
D M Y

3. _____
Amount & Currency

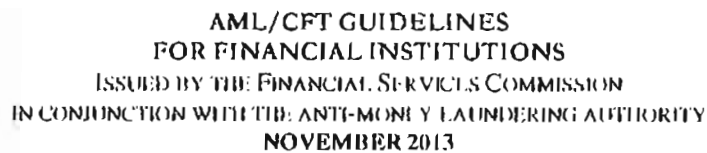
4. _____
BBD\$ Equivalent

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.



(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.)

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There is no handwriting or other markings on the paper.

PART E3

Anti-Money Laundering/Combating Terrorist Financing Guideline



**AML/CFT GUIDELINES
FOR FINANCIAL INSTITUTIONS**
ISSUED BY THE FINANCIAL SERVICES COMMISSION
IN CONJUNCTION WITH THE ANTI-MONEY LAUNDERING AUTHORITY
NOVEMBER 2013

a description (e.g. sex, approximate age, height, build, ethnicity, complexion, etc.)

PART F – Details of financial institution/place of transaction

1. _____
Organisation
applicable

2. _____
Branch where transaction occurred if

3. _____
Name and Title of Reporting Officer

4. _____
Signature of Reporting Officer

5. _____
Dealers internal reference number

6. _____
Reporting Officer's direct telephone number

