
# MONEY LAUNDERING & THE FINANCING OF TERRORISM

# GUIDELINES FOR FINANCIAL INSTITUTIONS

## Update

**[ISSUED 9 APRIL 2010]**

**Director of the ONDCP and**
**The Supervisory Authority under the**
**Money Laundering (Prevention) Act 1996**
**O.N.D.C.P. Headquarters**
**Camp Blizard**
**Antigua, West Indies**
Telephone: 562-3255, (268) 462-5934
Fax: (268) 460-8818
email: ondcp@candw.ag

# NOTICE

**To All Financial Institutions**: TAKE NOTICE that pursuant to the powers of the Director of ONDCP under section 43 of the Prevention of Terrorism Act 2005 and the Supervisory Authority under section 11(vii) of the Money Laundering (Prevention) Act 1996, the Money Laundering & Financing of Terrorism Guidelines are hereby updated by the amendment annexed hereto.

The most significant amendment comprises the introduction of the section titled Part II — The Financing of Terrorism, dedicated to issues relating to terrorist financing. There is also the introduction of an additional section titled, Part III — Sector Specific Guidelines, for dealing with issues peculiar to certain categories of financial institution.

These amendments serve to better fine tune Antigua and Barbuda's AML/CFT regime in alignment with international standards and its commitments to recommendations of the Caribbean Financial Action Task Force.

**These amendments come into effect on 4 May 2010.**

9 April 2010

Lt. Col. Edward Croft, OBE, CAMS, MBA, plsc
Director of ONDCP and
Supervisory Authority under the
Money Laundering (Prevention) Act 1996

**ANNEX**

## UPDATE TO THE MONEY LAUNDERING AND FINANCING OF TERRORISM GUIDELINES issued 9 April 2010

**Amendments:**

**1. Amendment to Part I – Money Laundering**

**2. Insertion of Part II – The Financing of Terrorism**

**3. Insertion of Part III – Sector Specific Guidelines**

## AMENDMENT

The Money Laundering and Financing of Terrorism Guidelines, which may be referred to herein as the MLFTG or ML/FTG are hereby amended as follows:

1. The Money Laundering and Financing of Terrorism Guidelines shall now be composed of three major parts as follows:

**PART I - MONEY LAUNDERING**

This part comprises:

1. The Money Laundering Guidelines issued 9 September 2002;
2. all the updates to the MLFTG issued prior to 9 April 2010, including those of:
    - 26 February 2003
    - 29 January 2004
    - 6 April 2006
    - 31 July 2006
    - 20 July 2009

**PART II – FINANCING OF TERRORISM**
**PART III – SECTOR SPECIFIC GUIDELINES.**

In addition, the Supervisory Authority has also issued Supplemental Guidance as follows:

- Preparing an AML/CFT Annual Audit Report or Annual Review, issued 19 May 2008
- Handbook for Preparing Reports of Suspicious Activity, Significant Payments and Terrorist Property, issued 7 April 2010.

2. Part I of the MLFTG is amended in relation to “Timing of Verification Requirements” by inserting after paragraph 2.1.14 the following:

2.1.14A (1) Regulation 4(3)(c) of the MLPR provides for transactions to proceed where satisfactory evidence of identity has not been obtained provided it is in accordance with a direction from the Supervisory Authority.

(2) Financial institutions should note carefully, that where a business relationship or one-off transaction has commenced but satisfactory evidence of identity has not yet been obtained, then if a situation is involved ***where it is essential not to interrupt the normal conduct of business***, the financial institution may permit the customer to utilise the business relationship prior to the identification of the customer or beneficial owner provided that:

(a) verification occurs as soon as reasonably practicable
(b) the money laundering risks are effectively managed by the financial institution in accordance with established risk management principles and documented decisions. (See ML/FTG Part II , Chapter 1, paragraph 1.3 )

(c) the financial institution has obtained from the customer information on the customer's:

(i) Name

(ii) date of birth

(iii) place of birth.

(3) Situations where it may be essential not to interrupt the normal conduct of business are:

(a) Life insurance business in relation to identification of the beneficiary under the policy. Identification and verification should take place in all cases at or before the payout or the time when the beneficiary intends to exercise vested rights under the policy.

(b) Securities transactions, where it is required to perform transactions very rapidly according to market conditions at the time the customer is contacting the financial institution, and performance of transaction is required before verification of identity is completed;

(c) Non face-to-face business;

3. There is inserted after Part I of the MLFTG the updater pages that immediately follow this page. These pages consist of the two new parts to the MLFTG which are titled respectively, Part II — Financing of Terrorism, and Part III — Sector Specific Guidelines.

**4. These Guidelines shall come into force on 4 May 2010. Financial institutions are encouraged to familiarize themselves with the new requirements and adopt them at an early opportunity and to provide comments and feedback to the Supervisory Authority prior to them coming into force.**

# UPDATER PAGES

# PART II — THE FINANCING OF TERRORISM

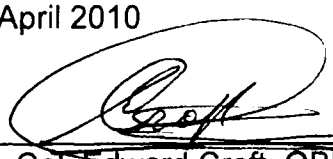
## From the Director of ONDCP and Supervisory Authority

Antigua and Barbuda, like other financial centers, faces the risk that its financial facilities could be used to facilitate the financing of terrorism. To date, there have been no reports that have warranted a full investigation into terrorist financing by the ONDCP. That, however, constitutes no basis for financial institutions to be less than fully cognizant of the potential of this threat and no basis to make less than a fully concerted effort to comply with obligations under the law to counter terrorism financing, to report the possession or control of terrorist property, to exercise all requisite due diligence and report financial transactions suspected of being related to terrorist financing and customers or persons suspected of being terrorist financers.

Therefore, financial institutions should take all required steps and implement all necessary and appropriate procedures to counter the financing of terrorism. There is need for the appropriate and effective dedication of resources to the problem. For these reasons, guidance is being provided on the risk-based assessment of customers and financial products as they relate to the risk of terrorist financing.

The effort to deal with the financing of terrorism is one that the ONDCP necessarily undertakes in partnership with financial institutions. The guidelines being issued on this important area of financial crime are designed to provide assistance to financial institutions in orienting themselves to the issues and procedural responses necessary to properly counter this threat.

9 April 2010



Lt. Col. Edward Croft, OBE, CAMS, MBA
Director of ONDCP and
Supervisory Authority under the
Money Laundering (Prevention) Act 1996

# FINANCING OF TERRORISM
# GUIDELINES FOR FINANCIAL INSTITUTIONS

## PREFACE

The Prevention of Terrorism Act 2005 sets out the obligation for financial institutions to be vigilant against having their facilities used for the financing of terrorism or as the repository of terrorist property, and to take necessary steps to counter these potential abuses of the legitimate financial system. Many of the procedures that will be appropriate to address these obligations are similar to the ones already established for countering money laundering, and financial institutions can often employ the same systems and controls to address them.

*The Money Laundering and Financing of Terrorism Guideline (MLFTG)* is now formatted in three parts: Part I contains the already established guidance on deterring, detecting and reporting money laundering. Part II contains guidance on deterring, detecting and reporting the financing of terrorism, and Part III contains sector specific guidance.

The Guidelines which comprise Part II of the *MLFTG* are designed to explain or clarify the procedures that should be taken in relation to the financing of terrorism that significantly differ from those used against money laundering or those procedures that are peculiar to dealing with the financing of terrorism. Where considered necessary, they amplify the guidance on money laundering.

Therefore, these Guidelines are incomplete on their own. They must be read in conjunction with the main guidelines on money laundering set out in Part I of the *Money Laundering and Financing of Terrorism Guidelines* issued by the Supervisory Authority. This is particularly important as the transactions and activities relating to the financing of terrorism can at times be indistinguishable from those related to money laundering. As such, the precautions to be taken against money laundering are an integral part of the precautions that are required to be taken against the financing of terrorism, and the Guidelines should be read with that in mind.

These Guidelines supersede all previous guidance on countering the Financing of Terrorism.

## INTRODUCTION

### Purpose of Guidance

The Purpose of these Guidelines is not to reproduce the requirements of anti-money laundering (AML) procedures [see Part I of the Guidelines], but to flag and focus attention and provide guidance on understanding and dealing with the aspects of the financing of terrorism that are distinct or distinguishable from money laundering in nature, appearance, modus operandi and procedure. It will also be important to indicate those procedures that are similar or identical to those required for dealing with money laundering. This will often be done by a simple citation to the money laundering provisions already contained in Part I of the Guidelines.

### To whom are these guidelines addressed?

Though financial institutions are designated differently under the MLPA for money laundering purposes and under the PTA for financing of terrorism purposes, it should be noted that without exception, all businesses designated as financial institutions under the PTA are also designated as financial institutions under the MLPA, though not the reverse. Under the PTA,

> *"financial institution" means a commercial bank, or any other institution which makes loans advances or investments or accepts deposits of money from the public."*

As such the money laundering requirements for customer due diligence, record keeping, reporting and training will remain fundamentally but not entirely the same. The guidance will be most important to senior management and compliance officers in financial institutions. It is expected to be likely that operational and frontline staff will be guided by the financial institution's often more detailed and more specific internal controls, policies and procedures.

### Scope of the Guidance

These Guidelines set out what is expected of financial institutions and their staff in relation to the prevention, detection and reporting of the financing of terrorism and the possession of terrorist property. These Guidelines relate to how financial institutions fulfill their obligations under the laws and regulations for countering the financing of terrorism.

Due to the many similarities between money laundering (with its close link to fraud) and terrorist financing, financial institutions should review their procedures against fraud and how these might reinforce each other.

These Guidelines establish a best practice for financial institutions in relation to the financing of terrorism. Departures from these recommendations and the rationale for doing so should be documented and may have to be justified in legal proceedings. Where financial institutions are subject to higher AML/CFT standards, then they are obligated to follow the higher standard.

**Terrorism Financing — Distinguishing FT from ML**

There can be considerable similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organized criminal activity. However, there are two major differences between terrorist property and criminal property generally:

- Often only small amounts are required to commit individual terrorist acts, thus increasing the difficulty of tracking the terrorist property;
- Terrorists can be funded from legitimately obtained income, including charitable donations, and it is extremely difficult to identify the stage at which legitimate funds become terrorist property.

Terrorist organizations can however, need quite significant funding and property to resource their infrastructure. They often control property and funds from a variety of sources and employ modern techniques to manage these funds, and to move them between jurisdictions.

In combating terrorist financing, the obligations on financial institutions is to report to the Director of ONDCP any suspicious activity relating to financing of terrorism and any property identified as being held or controlled for the benefit of a terrorist or financier of terrorism. This supports the aims of the law enforcement agencies in relation to the financing of terrorism, by allowing the freezing of property where there are reasonable grounds for suspecting that such property could be used to finance terrorist activity, and depriving terrorists of this property when links are established between the property and terrorists or terrorist activity.

**Terrorism Financing — Offences**

The Prevention of Terrorism (Amendment) Act 2008 defines terrorism financing to include “without limiting the generality, such conduct as is prohibited by sections 6, 7, 8, 9 and 10 of this Act.” The sections mentioned relate to the following:

- Section 6 – Provision or collection of funds to commit terrorist acts
- Section 7 – Collection of property or provision of property and services for commission of terrorist acts
- Section 8 – Use of property for commission of terrorist acts
- Section 9 – Money laundering [relating to terrorism]
- Section 10 – Soliciting and giving of support to terrorist groups or for the commission of terrorist acts.

A financial institution must not provide financial services to terrorists and their affiliates and has an obligation to take reasonable steps to avoid unwittingly facilitating any of the abovementioned offences.

**Obligations of Financial Institutions**

The obligation of financial institutions with respect to countering the financing of terrorism are outlined in Chapters I to V following.

**Abbreviations**

Much use is made of abbreviations in these Guidelines. An explanation of abbreviations can be found in at the end of Part II before the Appendices.

## About the Financing of Terrorism[1]

Terrorist financing is in principle different from money laundering, even although once such funds are in the financial system, they may be laundered in the same sorts of ways. Financial support for terrorist activities may come direct from certain states or jurisdictions, or from organizations large enough to be able to collect and make the funds available to the terrorist organization.

Terrorist organizations may engage in 'revenue-generating' activities of their own, which often in themselves may be, or certainly appear to be, legitimate businesses. Some of these activities, however, may include criminal acts and, to this extent, they may appear similar to 'ordinary' criminal organizations. Unlike other criminal organizations, however, terrorist groups may derive some of their funding from individuals and entities that have legitimately earned income. How much of a role 'legitimate' funds play in the support of terrorism seems to vary according to the terrorist group. Such a source of funds need not be, and often is not, in the same geographical location as that in which the terrorist organization commits its terrorist acts.

Much of the fight against terrorist financing turns on recognizing an involvement with persons or entities that have been defined, by governments or other international authorities, as having some connection with terrorism. Given the difficulty in knowing the true beneficiary of transactions, especially cross-border transactions, and the fact that terrorism often involves relatively small individual amounts, patterns of transactions or behaviour that might give clues to unusual underlying activity, are much more difficult to detect, even with the aid of computer modeling. Identifying the point at which legitimate customer funds are diverted to terrorist financing is well nigh beyond definition. Only by knowing their customers, and by looking out for every possible clue, can financial institutions have a chance to pick this up.

There is evidence that terrorists use traditional methods of money transmission such as Hawala to move funds between jurisdictions. Such transactions often involve transmission from one country through a third country, further obscuring the ultimate destination of the funds.

### 1. Apparently legitimate sources of terrorist financing

Because many terrorist movements have an ideological rational, individual terrorists or terrorist groups may sometimes be able to rely on legitimately generated sources of income. As mentioned above, this is a key difference between terrorist groups and traditional criminal organizations. Some fundraising methods specifically used by terrorist groups include:

- Collection of membership dues and/or subscriptions;
- Sale of publications, cassettes and other items;
- Speaking tours, cultural and social events;

---

[1] Source: Joint Money Laundering Steering Group
http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=774&a=9904

- Door-to-door solicitation within the community;
- Appeals to wealthy members of the community; and
- Donations of a portion of their personal earnings.

It is common practice within many religious communities to encourage a donation of a percentage of one's income to charity. There should be no automatic assumption that such donations bear any relation to terrorist financing. However, donations, often made on a regular basis, continue to be a lucrative source of funds from private individuals, certain states/jurisdictions, and from the sale of publications. Sometimes, large donations made by wealthy individuals in certain countries to organizations, are less associated with terrorism than with extortion, such as Mafia-style protection payments, where a 'donation' ensures that the donor's business interests remain allowed to operate.

**2. Non-legitimate sources of terrorist financing**

Criminality provides a much more consistent revenue stream to terrorist organizations. They will often choose activities that carry low risks and generate large returns . Major sources of income are:

- **Kidnapping and extortion;**
- **Fraud, including cheque and credit card fraud;**
- **Drug trafficking;**

  Raising funds in this way continues to be one of the most prolific and highly profitable means. Monies are usually raised from within the community of which the terrorists are an integral part. Eventually, extortion can become a built in cost of running a business within the community and the payment of ransom demands in order to free family members can become an every-day occurrence.

  Drugs can be a highly profitable source of funds and are used by some groups to finance other activities. Many terrorist groups are not directly involved in the importation or distribution of drugs, but in order for the suppliers to be allowed to operate within a certain area or community, a terrorist group can require some form a levy to be paid.

  Combating the supply of controlled narcotic substances is a high priority of virtually all law enforcement agencies throughout the world, and large resources are dedicated to investigation. Extortion is therefore far less risky than being responsible for organizing the supply and distribution of drugs.

  There are perhaps two distinct models for the involvement of terrorists in drugs. In the first, there is an antagonistic relationship between traffickers and terrorists; terrorists kidnap traffickers relatives for ransom, terrorists extort 'protection money' from traffickers, terrorists provide 'protection' for traffickers. In the second model, terrorists engage directly in the productions and trafficking of narcotics to raise money.

- **Smuggling**

  The profits made from smuggling can be channeled via couriers to another jurisdiction. Cash can enter the banking system through front companies or short-term shell companies that disappear after a few months. Specialized bureaux de change may also be created, whose sole purpose is the laundering of proceeds of smuggling.

  Another method of integrating the proceeds into the banking system is where monies are given by the smuggler to legitimate businesses not associated with the smuggling operation. These monies are then paid into the banking system as part of a company's normal turnover. Provided individuals are not greedy, detection is extremely difficult. Monies are then sent via different financial institutions and jurisdictions, including FATF blacklisted countries. The transfer of monies through different jurisdictions causes one of the principle problems of tracing the assets trail. Different legislative laws and procedures can prevent quick and effective investigation.

- **Misuse of Non-Profit Organizations and Charities**

  NPOs can be established in a wide variety of legal forms and are subject to varying degrees of control and monitoring by the jurisdictions in which they are located. Given their diversity, FATF has adopted a definition of NPOs which is based on their function rather than on their legal form.[2]

  The misuse of NPOs by terrorist groups can take many forms. One possibility is the establishment of an NPO with a stated charitable purpose, but which actually exists only to channel funds to a terrorist organization. Another possibility is that an NPO with a humanitarian or charitable purpose is infiltrated by the terrorists and their supporters, often without the knowledge of the donors, or the members of staff, or management. Still another possibility is for the organization to serve as the intermediary or cover for the movement of funds, usually on an international basis. In some cases, the NPO support function could extend to the movement and logistical support of the terrorists themselves.

**3. Laundering through the financial system**

Whilst terrorist groups may support themselves with funding from legitimate and non-legitimate sources, there appears to be little difference in the methods used by terrorist groups or criminal organizations to hide or obscure the links between the source of the funds and their eventual destinations or purposes.

Bank accounts have been used in the following manner to launder terrorist funds:

- **Legitimate accounts**

---

[2] Any legal entity that engages in the raising or disbursing of funds for charitable, religious, cultural, educational, social, fraternal or humanitarian purposes, or for the purposes of carrying out some other types of good works.

Individuals may run a number of accounts with several banks. It is not unusual for the accounts with one bank to be used for domestic purposes, while accounts based at another are for 'business purposes'. In the former, a salary or benefits may be paid, while the latter account will be used for money transfers and cheque payments.

- **Dormant accounts**

  On occasions, dormant accounts have been used by terrorists to create a purported customer relationship, upon which additional frauds may be perpetrated. Facilities can be accessed, including bank loans, the repayment installments of which will invariably not be met.

  Dormant accounts have also been used to receive monies from support members abroad. In one example, a terrorist used a number of banks, holding an account in each of them. Two of the accounts contained a minimal sum, believed to be for two purposes: first, to keep the account open, and secondly, to ensure that undue attention was not drawn to it. At a strategic time, a transfer was received into the account, to enable the purchase of terrorist material. The sum was eroded by the daily removal of the maximum cash amount from automatic teller machines. This continued until the entire transfer sum had been removed, which took almost two months.

- **Telegraphic transfers**

  These can be effected through banks or wire transfer companies. The experience of law enforcement suggests that banks or wire transfer companies based in retail outlets containing video cameras are used to a much lesser extent than those where the wire transfer service is franchised to a small, more localized unit. However, the extent to which these facilities are used is also determined by the ease of both sending and receiving the money. In cases where companies do not request documentation, and require only the use of a pre-agreed question and answer prior to the release of the transferred sum, these facilities are particularly attractive to money launderers.

- **Money service businesses and alternative remittance systems**

  Given that many sources of terrorist funding (for example, extortion and drug trafficking) generate a high volume of cash, terrorists often channel funds through bureaux de change, money changers and other dealers in foreign currency to finance their operations abroad. Money may pass through several jurisdictions before reaching its final destination.

- **Poorly regulated jurisdictions**

  Terrorists may choose to locate bank accounts in jurisdictions with a low level of effective regulation. Transfers out of, or in to, such jurisdictions are difficult to follow through, thus creating a 'dead end' for financial investigators.

# Chapter I: POLICIES, CONTROLS AND PROCEDURES

*This guidance is incomplete on its own — It must be read together with Section 1 of Part I of the MLFTG on money laundering and the updates thereto.*

*This chapter provides guidance on the general policies and controls that a financial institution needs to put in place and maintain to counter terrorism financing and associated money laundering, which will shape the procedures that are developed and provided for frontline and operational staff to implement.*

**Legal framework**

PTA 41B
MLPR 3(1), 3(1)(c)(ii), 3(7), 15

## 1.1 Designers and Implementers of AML/CFT Policy

### A. SENIOR MANAGEMENT

---

**Core Obligations:**

- Appoint a compliance officer with certain responsibilities
- Devote adequate resources to AML/CFT
- Potential personal liability if obligations not met

---

**Actions required and subject to regular review:**

- Prepare a formal written policy in relation to terrorist financing
- Ensure adequate resources are devoted to AML/CFT
- Commission an AML/CFT annual review and take necessary action to remedy deficiencies identified by the report

---

1.1.1 A financial institution must not allow itself and its facilities to be used for the purposes of crime (money laundering) or terrorist activity (terrorism financing). This must neither be done deliberately, by turning a blind eye or negligently, by failing to have appropriate procedures to counter these activities. All the supervisory provisions of the Money Laundering (Prevention) Act and the Prevention of Terrorism Act are aimed at shielding and buffering financial institutions, the financial sector and ultimately the jurisdiction from becoming the repository or facilitator of criminal proceeds. The responsibility for being vigilante against the criminal abuse of a financial institution's facilities rests primarily on the senior management of the financial institution. The Prevention of Terrorism

(Amendment) Act 2010 makes this clear in how it places responsibility in section 41B:

> "**41B Liability of Directors, etc. where offence committed by body corporate.**
> Where a body corporate commits an offence under this Act, every director or other officer concerned in the management of the body corporate commits that offence unless he proves that -
> (a) the offence was committed without his consent or connivance; and
> (b) he exercised reasonable diligence to prevent the commission of the offence."

1.1.2 Senior management has a responsibility to ensure that a financial institution's control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the financial institution being used in connection with the financing of terrorism as well as money laundering.

1.1.3 In banks and other traditional financial institutions senior management is accustomed to apply proportionate risk-based policies across different aspects of the business. Financial institutions are required to take such an approach to the risk of being used for the purposes of terrorist financing.

1.1.4 Under a risk-based approach, financial institutions in Antigua and Barbuda may tend to start with an assumption that their customers are unlikely to be terrorist financiers or the holders or controllers of terrorist property. (Up to March 2010 there had not been a SAR or report of terrorist property in the jurisdiction that required a full investigation or prosecution.) Nonetheless, the law requires that financial institutions have proportionately robust systems in place to detect specified entities (terrorists) and their property, and to highlight those customers who, on criteria established by the financial institution, may indicate that they present a risk of being financiers of terrorism or terrorism-related money launderers. The systems and procedures should be proportionate to the risks involved, and should be cost effective.

1.1.5 Senior management must be fully engaged in the decision making processes, and must take ownership of the risk-based approach, since they will be held accountable if the approach is inadequate.

1.1.6 The Money Laundering (Prevention) Act and Regulations apply to all business activities listed in the First Schedule to the MLPA, which are termed "financial institutions". The Prevention of Terrorism Act extended the scope of AML legislation to apply it to any dealings in criminal or terrorist property. Thus in considering their statutory obligations financial institutions need to think in terms of involvement with any crime or terrorist activity.

1.1.7 Therefore, it is for senior management to ensure that written policies on how terrorist financing and related money laundering matters are to be dealt with by the institution are drafted, published, made available to staff and implemented.

1.1.8 Training is important and financial institutions have an obligation under the MLPR to take appropriate measures so that employees are made aware of the relevant provisions of the Regulations and the Prevention of Terrorism Act.

1.1.9 Senior management must appoint a compliance officer at management level to handle terrorism financing matters. They must also ensure that the compliance officer is adequately trained and resourced.

1.1.10 The role, standing and competence of the compliance officer, and the way the internal processes for reporting suspicions are designed and implemented, impact directly on a financial institution's terrorist financing prevention arrangements.

1.1.11 It is for senior management to commission and provide for an annual assessment of the effectiveness of the AML/CFT system of the financial institution, pursuant to the MLPR, reg. 15. The assessment by senior management of the outcome of the annual AML/CFT system review is critical to how the financial institution adapts to changing circumstances and innovations in the criminal community and assures the adequacy of its counter-measures. Annual reviews are mandatory even where there is reason to believe that there will not be a need for any consequent modification of the system.

## B. COMPLIANCE OFFICERS

**Legal framework**
**Regulations**
MLPR regulation 6(1)
**Guidelines**
MLFTG Part I, Section 1, paras. 1.0, 1.1, I.2(III)
**International standard:**
FATF Recommendation 5

---

**Core obligations:**

- Receive and review internal suspicious activity reports
- Make external suspicious activity reports
- Competence required
- Should be able to act on own authority with respect to AML/CFT matters
- Adequately resourced
- Responsible for oversight of the financial institution's compliance with its requirement for AML/CFT staff training

---

**Actions required and subject to regular review:**

- Senior management should ensure that the compliance officer has:
  - Support of senior management
  - Adequate resources

  - Independence of action
  - Access to information
  - Responsibility for financial institutions compliance with its requirements for AML/CFT staff training
  - Participates in production of annual AML/CFT review or report
- Compliance officer required to ensure he/she has continuing competence
- Compliance officer to monitor the effectiveness of systems and controls

---

**General legal and regulatory obligations**
[See MLFTG Part I, Section 1 paragraph 1.0 et seq.]

1.1.12 A person at management level should be appointed the compliance officer for matters relating to the financing of terrorism and the reporting of terrorist property. The financial institution should have in place a compliance officer for money laundering and may choose to appoint the same person to be the FT compliance officer or assign those duties to a separate person.

1.1.13 There are advantages to the ML and FT compliance officer being the same person in that it avoids the duplication of duties and costs since the person responsible for FT will likely be responsible for money laundering related to FT, which in itself is not different from ordinary ML.

1.1.14 If the compliance officer for ML is different from the officer responsible for FT, arrangements should be made to ensure that where necessary the two are able to communicate effectively with each other for the sharing of information that will enhance and supplement their individual duties.

**Internal and external suspicious activity reporting**
[See MLFTG Part I, Section 4 paragraph 4.12 – 4.16, MLPR regulation 6]

1.1.15 A financial institution should take reasonable steps to ensure that an internal report of possible ML or FT is considered by the compliance officer as soon as is reasonably possible.

1.1.16 An internal report should be considered by the compliance officer in the light of all other relevant information to determine whether or not the information contained in the report does give rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of ML or FT.

1.1.17 A financial institution is expected to use its existing customer information effectively by making such information readily available to its compliance officer as needed for his/her duties.

1.1.18 In most cases, before deciding to make a report to the Supervisory Authority or Director of the ONDCP, the compliance officer is likely to need access to the financial institution's relevant business information. A financial institution should therefore take reasonable steps to give its compliance officer access to such information. Relevant business information may include details of:

the financial circumstances of a customer or any person on whose

behalf the customer has been or is acting; and

the features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place, which the financial institution entered into with or for the customer (or that person).

In addition, the compliance officer may wish:

- to consider the level of identity information held on the customer, and any information on his personal circumstances that might be available to the financial institution; and
- to review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

1.1.19 If the compliance officer concludes that the internal report does give rise to knowledge or suspicion of ML or FT, he must make a report to the Supervisory Authority or Director of the ONDCP.

1.1.20 Guidance on making external reports to the Director of the ONDCP is set out in Chapter 4.

**Monitoring effectiveness of AML/CFT controls**

1.1.21 A financial institution should carry out an annual AML/CFT system review to assess the adequacy of the systems and controls to ensure that they manage the FT risk effectively. The compliance officer should take an active part in this exercise.

**Reporting to senior management**

1.1.22 At least annually the compliance officer should submit a report to senior management which gives his/her assessment of the operation and effectiveness of the financial institution's systems and controls in relation to managing FT risks.

## 1.2 INTERNAL CONTROLS

*This section provides guidance on the internal controls that will help financial institutions meet their obligations in respect of the prevention of money laundering and the financing terrorism.*

**Legal framework**
**Regulations**
MLPR regulation 3(1)
**Guidelines**
MLFTG Section 1
**International standard:**
FATF Recommendation 15

**Core obligations**

- Establish and maintain appropriate procedures to forestall and prevent terrorism financing
- Institute controls sensitive to the risks faced by the financial institution

**Actions required to be taken and kept under regular review**

- Establish and maintain appropriate procedures to forestall and prevent terrorism financing
- Institute controls sensitive to the risks faced by the financial institution
- Maintain appropriate control and oversight over outsourced activity

**General legal obligations**

[See MLFTG Part I, Section 1]

1.2.1 Financial institutions are required to develop, implement and maintain written internal policies, controls and procedures for recognizing and dealing with transactions, and attempted and proposed transactions relating to terrorism and the financing of terrorism, whether by persons or entities declared to be specified entities, suspected of being terrorist entities or affiliates or financiers of terrorism.

1.2.2 There are specific requirements under the ML Regulations (reg. 3) for a financial institution to have procedures in place in relation to:

customer identification;

record keeping;

reporting of suspicious activities;

staff awareness and training;

hiring staff;

annual review and audit reports.

1.2.3 An aspect of the nature of the financing of terrorism, is that FT, because financial transaction may involved, is likely to take place with ML also occurring at some point. Therefore, financial institutions are required to have systems and controls appropriate to their business, which must include measures for countering the risk that the financial institution might be used to further financial crime generally. Financial crime includes the handling of the proceeds of crime — that is money laundering or terrorist financing. The nature and extent of systems and controls of the financial instituion will depend on a variety of factors, including:

- the nature, scale and complexity of the financial institution's business
- its customer, product and activity profile

- the volume and size of its transactions
- and the degree of risk associated with each area of its operations.

1.2.4 If financial institutions outsource some of their systems and controls to third parties. this brings an additional dimension to the risks faced which must be **actively** managed.

1.2.5 Financial institutions cannot contract out of their regulatory responsibilities and therefore remain responsible for systems and controls in relation to the activities outsourced.

## 1.3 RISK BASED APPROACH

---

**Core obligations:**

- Systems and controls should reflect the degree of risk associated with the business and its customers
- Take into account the greater potential for terrorist financing and money laundering related to FT which arises when the customer is not physically present

---

**Actions required and subject to regular review:**

- Carry out regular AML/CFT risk assessment, which should include assessment of market changes, and changes in products, customers and the wider environment
- Ensure internal procedures, systems and controls, including staff awareness, adequately reflect the risk assessment
- Ensure customer identification and acceptance procedures reflect the risk characteristics of customers
- Ensure arrangements for monitoring systems and controls are robust, and reflect the risk characteristics of customers

---

### 1.3.1 Introduction

(1) Financial institutions should adopt a risk-based approach for dealing with Financing of Terrorism threats. The purpose of this is not to introduce a less stringent form of customer due diligence, but to encourage financial institutions to efficiently **allocate resources according to the degree of assessed risk.** Therefore, though a risk-based approach would result in less scrutiny being applied to certain customers, this cannot be done unless a proper risk assessment has been conducted of the customer and the product the customer wishes to make use of. Any risk assessment must be documented and be available to Regulators and as appropriate to the Supervisory Authority.

Enforcement action will be taken where an inadequate risk assessment has been done.

(2) Under a risk-based approach, a financial institution must take a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the risks of FT and related ML that it faces and design and implement controls to manage and reduce those risks. Briefly, these steps are to:

- Identify the FT and ML-related risks that are relevant to the financial institution
- Assess the risks presented by the institution's particular

customers;

products' delivery channels; and

geographical areas of operation;

- Design and implement controls to manage an mitigate these assessed risks
- Monitor and improve the effective operation of these controls
- Record appropriately what has been done and why.

**1.3.2 Identifying and assessing the risks faced by financial institutions**

(1) A financial institution should assess its risks in the context of how it might most likely be involved in money laundering or terrorist financing. In this respect, senior management should ask themselves a number of questions:—

- What risk is posed by the customers? For example:
  - complex business ownerships structures, which can make it easier to conceal underlying beneficiaries
  - PEP
  - Customers based in or conducting business in high risk jurisdictions
  - Customers engaged in business which involves a significant amount of cash.
- What risk is posed by a customer's behaviour. For example
  - Where there is no commercial rational for the customer buying the product he seeks;
  - requests to associate undue levels of secrecy with a transaction;
  - situations where the origin of wealth and/or source of funds cannot be easily verified or where the audit trail has been deliberately broken and/or unnecessarily layered; and
  - the unwillingness of non-personal customers to give names of their real owners and controllers.
- How does the way the customer comes to the financial institution affect the risk?
  - one-off transactions versus business relationships
  - introduced business, depending on the effectiveness of the due diligence carried out by the introducer; and

- non face-to-face acceptance.

- What risk is posed by the products/services the customer is using. For example:
  - Can the product features be used for ML or FG, or to fund other crime/
  - do the products allow/facilitate payments to third parties?
  - is the main risk that of inappropriate assets being placed with, or moving from, or through the financial institution?
  - does a customer migrating from one product to another within the financial institution carry a risk?

**1.3.3 Design and implement controls to manage and mitigate the risks**

(1) To decide on the most appropriate and relevant controls for the financial institution, senior management should ask themselves what measures the financial institution can adopt, and to what extent, to manage and mitigate these threats/risks most cost effectively, and in line with the financial institution's risk appetite. Examples of control procedures include:

- Introduce a customer identification program that varies the procedures in respect of customers appropriate to their assessed FT risk;
- Obtaining additional customer information where appropriate to the level of assessed FT risk
- Monitoring customer transactions/activities

A customer identification program that is graduated to reflect risk could involve:

- a standard information dataset to be held in respect of all customers;
- a standard verification requirement for all customers;
- more extensive due diligence on customer acceptance for higher risk customers (i.e. more identification checks and/or requiring additional KYC information);
- where appropriate, more limited identity verification measures for specific lower risk customers/product combinations; and
- an approach to monitoring customer activities and transactions that reflects the risk assessed to be presented by the customer, which will identify those transactions or activities that may be unusual or suspicious.

(2) In assessing customer risk consideration should be given to all information obtained as part of the normal vetting process.

(3) Identifying a customer as carrying a higher risk of FT does not automatically mean that he is a financier of terrorism. Similarly, identifying a customer as carrying a low risk of FT does not mean that the customer is not. Staff therefore need to be vigilant in using their experience and common sense in applying the financial institution's risk-based criteria and rules.

### 1.3.4 Monitor and improve the effective operation of controls

A financial institution will need to have some means of assessing that its risk mitigation procedures and controls are working effectively, or, if they are not, where they need to be improved. Consideration will need to be given to:

- Appropriate procedures to identify changes in customer characteristics, which come to light in the normal course of business;
- Reviewing ways in which different products and services may be used for financing of terrorism purposes, and how these ways may change, supported by typologies
- Adequacy of staff training
- Monitoring compliance arrangements (such an audits and reviews)
- The balance between technology-based and people-based systems
- Upward reporting and accountability
- Effectiveness of liaison with other parts of the financial institution
- Effectiveness of the liaison with regulatory and law enforcement agencies.

### 1.3.5 Record what has been done and why

A financial institution must document:

- how it assesses the threats/risks of being used in connection with terrorist financing;
- how it agrees and implements the appropriate systems and procedures, including due diligence requirements, in the light of its risk assessment;
- how it monitors and, as necessary improves the effectiveness of its systems and procedures; and
- the arrangements for reporting to senior management on the operation of its control processes.

### 1.3.6 Risk management is dynamic

Risk management generally is a continuous process, carried out on a dynamic basis. A terrorist financing risk assessment is not a one-time exercise. Financial institutions should therefore ensure that their risk management processes for managing FT are kept under regular review.

# Chapter II: CUSTOMER DUE DILIGENCE

*This guidance is incomplete on its own — It must be read together with Section 2 of Part I of the MLFTG on money laundering and the updates thereto.*

*This chapter provides guidance on the critical procedures for identifying customers, verifying that a customer is who the customer purports to be, and the procedures for gathering further information in order to understand customer business and the purpose for which an account is opened, often referred to as Know Your Customer procedures or KYC.*

**Legal framework**

**Acts**

- PTA section 3(2), 4
- MLPA, section 11A, 18(1), 18(2)

**Regulations**

- MLPR regulations 3(1)(i), 4, 7
- IGIWR

**Guidelines**

- MLFTG Part I, section 2
- CDD Guidelines of the FSRC

**Customers that may not be dealt with**

- Specified Entities as declared by order of the Attorney General
- Specified Entities listed on the ONDCP website, www.ondcp.gov.ag

**International standard setter**

FATF SR VII

---

**Core obligations**

- Must have processes for identifying specified entities
- Must have processes for identifying different types of customers
- Procedures must take account of the greater potential for terrorist financing and related money laundering activity which arises when the customer is not physically present when being identified
- Some persons must not be dealt with
- If satisfactory evidence of identity is not obtained, the business relationship must not proceed further
- Must have a system for updating customer information

---

**Actions required or required to be kept under regular review**

- Must have system of ongoing due diligence
- Make monthly checks of the ONDCP website for listings and de-listings of Specified Entities

---

NOTE: All customer identification requirements and enhanced due diligence requirements for money laundering in Part I of the MLFTG must be implemented in relation to precautions against the financing of terrorism and transactions or attempted transactions that may be related to terrorist activity.

## 2.1 WHAT IS CUSTOMER DUE DILIGENCE? — (ID + KYC)

2.1.1 The obligation on financial institutions to be reasonably satisfied that their customers are who they say they are, and what to do if they appear to be acting on behalf of others, are set out in the MLPA and the MLPR. The obligations are designed to make it more difficult for the financial sector to be used for ML or FT.

2.1.2 Financial institutions need to carry out customer due diligence for two broad reasons:

- to help the financial institutions to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another and that there is no legal barrier (e.g. government prohibitions) to providing them with the product or service requested.
- to help law enforcement by providing information on customers or activities being investigated.

2.1.3 It may often be appropriate for a financial institution to know rather more about the customer than his identity: it will, for example, often need to be aware of the customer's business in order to assess the extent to which his transactions and activity undertaken with or through the financial institution is consistent with that business.

2.1.4 The due diligence carried out on new customers is in two distinct parts:

(1) verifying the customer's identity,

(2) in the risk-based approach, by obtaining additional information in respect of some customers to know your customer ("KYC").

**KYC** = obtaining appropriate additional information, includes understanding the customer's circumstances and business - including where appropriate, the source of funds, and in some cases the source of wealth and the purpose of specific transactions - and the expected nature and level of transactions; and

(3) keeping such information current and valid.

2.1.5 The amount and balance of resources applied to ID and KYC will reflect the ML or FT risk customers present, taking account of the nature of their business and geographical location, and of the product or service sought.

## 2.2 CUSTOMER IDENTIFICATION

### 2.2.1 Nature and proof of identity

[See MLFTG Part I, Section 2, paragraph 2.1.6]
Documentary evidence is required for proof of identity.

### 2.2.2 Initial identity checks

[See MLFTG Part I, Section 2, paragraph 2.1.7 – 2.1.16]

(1) Identifying a customer is a two-part process. The financial institution first *identifies* the customer, by obtaining a range of information from him. The second part — the *verification* — consists of the financial institution verifying some of this information through the use of reliable, independent source documents, data or information.

(2) The guidance in this section first addresses personal customers, and secondly non-personal customers. The guidance indicates the standard identification requirement, and then goes on to provide further guidance on steps that may be applied as part of a risk-based approach.

(3) The guidance in this section should be read in conjunction with that on the risk-based approach set out in Part II, Chapter 1, paragraph 1.3.

(4) The minimum information to be collected for the identification of a customer doing a one-off transaction, is as follows:

Personal customers:
(a) name
(b) residential address
(c) date of birth

Non personal customers:
(a) name
(b) business address
(c) name and address of person effecting the transaction

*Electronic transfer of funds*

(5) To implement FATF Special Recommendation VII, MLPR regulation 4(3)(m) (amended 2009) and MLFTG Part 1 paragraphs 3.4 – 3.13, require accurate and meaningful originator information.

### 2.2.3 PERSONAL CUSTOMERS

[See MLFTG Part I, Section 2, paragraph 2.1.17 – 2.1.13, 2.1.28]

### 2.2.4 Non face-to-face customers

[See MLFTG Part I, Section 2, paragraphs 2.1.23 – 2.1.27]

## 2.3 IDENTIFYING CUSTOMERS PROHIBITED FROM FINANCIAL SERVICES

Financial institutions must not provide services to persons who are *specified entities*. Property of such persons should be frozen upon receipt of the Attorney

General's declaration of a specified entity without undue delay in accordance with his directive.

**WHO ARE SPECIFIED ENTITIES?**

### 2.3.1 Declaration of Specified Entities

(1) A Specified Entity is a person declared by the Attorney General to be a specified entity. The PTA, section 3, provides for the Attorney General to make an Order declaring certain persons who are considered to be terrorist organizations, members of terrorist organizations or who have links to terrorist organizations to be specified entities.

(2) Under section 4(1) of the PTA Antigua and Barbuda is to give effect to the decisions of the United Nations Security Council on measures to be employed in relation to terrorism. This information will be available on the ONDCP website at www.ondcp.gov.ag.

### 2.3.2 Effects of the Declaration of Specified Entities

The making of a Declaration of a person to be a Specified Entity takes immediate effect upon the Attorney General signing the Order.

### 2.3.3 Communication of Declaration of Specified Entities

(1) The Attorney General is authorized by section 3(2B) of the PTA to communicate the Declaration to financial institutions by any appropriate means. The mode of communication may include fax, email and other documentary means.

(2) Financial institutions should be prepared to receive communication of details of specified entities by a Notice of Declaration. A copy of the form of the Notice of Declaration is contained in Appendix I, Form 1. The manager of a financial institution and in his absence the compliance officer should expect to ordinarily be the point of contact to whom information about a directive to freeze would be communicated.

(3) Financial institutions should have procedures in place for follow-up action to be taken without delay upon the receipt of communication of the Attorney General's order declaring a specified entity and any directive to freeze the entity's funds.

### 2.3.4 Action to be taken upon receipt of the Communication of a Declaration of Specified Entities

The PTA authorizes the Attorney General, by order, to give directions to financial institutions on how to deal with accounts and funds of persons declared to be specified entities. Such instructions may in the first instance be included as Directives that are part of the Order declaring specified entities contained in the Notice of Declaration of Specified Entities (See Appendix I, Form 1).
A Financial Institution upon receiving communication of the Notice of Declaration should as a minimum carry out the following standardized procedures:

(1) Treat as **confidential** the communication of a directive from the Attorney General to freeze the funds of a specified entity, and have staff deal with matters related to the declaration on a needs to know basis**.**

(2) Check without delay its customer database to determine whether the name of any Specified Entity listed in the Declaration matches that of any of its customers. Where names have been translated from original non-western alphabet then it may be appropriate to check not only the exact matches but also phonetic matches and spelling variations for a match;

(3) If a match is found freeze without delay any account or other property held by the financial institution for or on behalf of the Specified Entity;

(4) Make a Specified Entity Property Report to the Director of the ONDCP on the Specified Entity Reporting Form (See Appendix I, Form 3a or 3b).

(5) Comply with any further aspects of the Attorney General's Directive in relation to the Specified Entity.

### 2.3.5 Instructions from the Director of ONDCP

The Director of ONDCP publishes and updates the list of specified entities on the ondcp webiste: www.ondcp.gov.ag. Specified entities are subject to a sanction regime prohibiting the provision of financial services to them. Financial institutions should consult this list and take the same action set out in paragraph 2.3.4 above.

### 2.3.6 Searching the UN websites for listed entities

On a monthly basis, the compliance officer of a financial institution should:—

(1) visit the following websites:

- The United Nations Security Council 1267 Sanctions Subcommittee latest news at (click the link): http://www.un.org/sc/committees/1267/latest.shtml.
- The United Nations Security Council 1267 Sanctions Subcommittee Consolidated List of Persons and Entities at (click the link): http://www.un.org/sc/committees/1267/consolist.shtml.
- The United Nations Security Council 1267 Subcommittee list of Approved Amendments to the Consolidated List of Persons and Entities at the latest news website (see the first bullet above)
- The United Nations Security Council 1267 Subcommittee list of Persons and Entities Delisted from the Consolidated List at (click the link): http://www.un.org/sc/committees/1267/removed.shtml.

(2) Obtain information on the changes in the UN Consolidated List of Terrorists and Terrorist Entities.

(3) Information on the UN Consolidated List of Terrorists should also be available on the ONDCP website at www.ondcp.gov.ag.

### 2.3.7 Responding to matches between the UN List and the Customer database

(1) Record and report any matches between names on the list and customers of the financial institution, being careful to check that dates of birth also match. Also checking not only for exact matches but for close matches, particularly where other details match, such as date and place of birth etc.

(2) The Compliance Officer should then update the financial institution's list of specified entities by making appropriate changes to it in accord with the listing or delisting of persons and entities on the UN website or ONDCP website.

(3) If new names on the List are a match then without delay make a Specified Entity Property Report to the Director of the ONDCP.

(5) If names on the List are a match then invoke the freezing procedures for accounts and property in relation to the person, as set out in the internal controls of the financial institution and in accordance with the law.

(6) All new or potential customers should be checked against the names on the UN List.

### 2.4 Enhanced Due Diligence

[See MLPR regulation 4(3)(d)]
This concerns obtaining additional information beyond standard ID + KYC when dealing with high risk customers.

### 2.5 Ongoing Due Diligence

[See MLPR regulation 2 - Interpretation]
This regulation defines "ongoing due diligence" and concerns keeping customer information current and up-to-date.

### 2.6 NON-PERSONAL CUSTOMERS

#### 2.6.1 Corporations

[See MLFTG Part I, Section 2, paragraph 2.1.39]

##### 2.6.1.1Publicly quoted companies

(1) Corporate customers that are listed on a regulated market are publicly owned and generally accountable. Corporate customers that are subject to statutory licensing and regulation of their industry (for example, energy, telecommunications) may be considered to be similarly owned and accountable.

(2) Where the financial institution has satisfied itself that the customer is:
a publicly quoted company, subject to public disclosure rules; or
a majority-owned and consolidated subsidiary of such a publicly quoted company; or subject to the licensing and prudential regime of a statutory regulator (e.g. the SEC in the U.S. or OFCOM in the UK), it need take no further steps to verify identity over and above obtaining the standard evidence.

##### 2.6.1.2Private companies

(1) Unlike publicly quoted companies, the activities of private companies are often carried out for the profit/benefit of a small and defined groups of individuals or entities. In general, however, the structure, ownership, purposes and activities of many private companies will be clear and understandable.

(2) When private companies are well known, reputable organisations, with long histories in their industries and substantial public information about them, the standard evidence may well be sufficient to meet the financial institution's

obligations.

(3) Standards of control over the issue of documentation from company registries vary between different countries. Attention should be paid to the jurisdiction the documents originate form and the background against which they are produced.

(4) Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client identity, financial institutions should consider the money laundering or terrorist financing risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identities of the principal beneficial owners, shareholder and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the entity.

(5) Following the financial institution's assessment of the FT and ML risk presented by the company, the financial institution may feel it appropriate to verify the identity of appropriate beneficial owners holding 25% or more of the shares. Where a principal owner is another corporate entity or trust, the financial institution should take measures to look behind that company or trust and establish the identities of its beneficial owners or trustees, unless that company is publicly quoted. The financial institutions will then judge which of the beneficial owners exercise effective control, and whose identities should therefore be verified.

(6) Control may also rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms. Financial institutions should make an evaluation of the effective distribution of control in each case. What constitutes a significant shareholding or control for this purpose will depend on the nature of the company, the distributions of shareholdings, and the nature and extent of any business or family connections between the beneficial owners.

(7) Extra care must be taken in the case of companies with capital in the form of bearer shares, because in such cases it is often difficult to identify the beneficial owner(s).

### 2.6.2 Charities, Friendly Societies, Non Profit Organizations

(1) Charities have their status because of their purposes and can take a number of legal forms. If registered in Antigua and Barbuda they are registered under the Friendly Societies Act.

(2) In each case, a charity should be treated for AML/CFT purposes, and standard evidence obtained, according to its legal form.

(3) Financial institutions should take appropriate steps to be reasonably satisfied that the person the financial institution is dealing with is properly authorized by the customer and is who he says he is.

(4) Where an independent school or college is a registered charity, it should be treated in accordance with the guidance for charities. Any such body which is not registered as a charity should be treated in accordance with the guidance for private companies in paragraph 2.6.1.2

*Variation from the standard*
(5) The identities of unregistered charities or church bodies, whether in Antigua and Barbuda or elsewhere, cannot be verified by reference to a register maintained by independent bodies. Applications from, or on behalf of, unregistered charities should therefore be dealt with in accordance with the procedures for private companies set out in paragraphs 2.6.1.2, for trusts, as set out in paragraphs 2.6.3, for clubs and societies as set out in paragraphs 2.6.5 Financial institution should take particular note of those paragraphs addressing customers where the terrorist financing and associated money laundering risk is greater in relation to particular customers, and if it should be followed in these circumstances.

(6) In assessing the risks presented by different charities, a financial institution should make appropriate distinction between those with a limited geographical remit; and those with unlimited geographical scope, such as medical and emergency relief charities.

(7) If they have a defined area of benefit, charities are only able to expend their funds within that defined area. If this area is an overseas country or jurisdiction, the charity can quite properly be transferring funds to that country or jurisdiction. It would be less clear why the organization should be transferring funds to a third country (which may, within the general context of the financial institution's risk assessment have a lower profile) and this would therefore be unusual. Such activity would lead to the charity being regarded as high risk.

(8) Non profit organizations have been known to be abused, to divert funds to terrorist financing and other criminal activities.

### 2.6.3 Other trusts, foundations and similar entities

(1) There is a wide variety of trusts, ranging from large, internationally active organisations subject to a high degree of public interest and quasi-accountability, through trusts set up under testamentary arrangements, to small, local trusts funded by small, individual donations from local communities, serving local needs. It is important, in putting proportionate AML/CFT processes into place, and in carrying out their risk assessments, that financial institutions take account of the different money laundering or terrorist financing risks that trusts of different sizes and areas of activity present.

(2) Most trusts are not separate legal entities - it is the trustees collectively who are the customer, In these cases, the obligation to identify the customer attaches to the trustees, rather than to the trust itself. The purpose and objects of most trusts are set out in a trust deed.

(3) In respect of trusts, the financial institution should obtain the following information:

full name of the trust
nature and purpose of the trust (e.g., discretionary, testamentary, bare)
country of establishment
names of all trustees
name and address of any protector or controller

(4) The financial institution should verify the identities of the trustees (or equivalent) who have authority to operate an account or to give the financial institution instructions concerning the use or transfer of funds or assets.

(5) Where the trustee is itself a regulated entity or a publicly quoted company, or other type of entity the identification procedures that should be carried out should reflect the standard approach for such an entity.

(6) Financial institutions should take appropriate steps to be reasonably satisfied that the person the financial institution is dealing with is properly authorised by the customer and is who he says he is.

(7) Some consideration should be given as to whether documents relied upon are forged, In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity

### 2.6.4 Partnerships and other unincorporated businesses

(1) Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from personal customers in that there is an underlying business. This business is likely to have a different money laundering or terrorist financing risk profile from that of an individual.
Where partnerships and unincorporated businesses are well known, reputable organizations, with long histories in their industries, and with substantial public information about them and their principals and controllers, the standard evidenced for publicly quoted companies will be sufficient to meet the financial institution’s obligations.

(2) Professional firms that are partnerships, and that are subject to the ML Regulations should be treated as under paragraph 2.6.4.

(3) Other partnerships and unincorporated businesses should be treated as private companies, as set out in paragraph 2.6.1.2.

(4) Financial institutions should take appropriate steps to be reasonably satisfied that the person the financial institution is dealing with is properly authorized by the customer and is who he says he is.

(5) Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer’s identity.

*Variation from the standard*

(6) Most partnerships and unincorporated businesses are smaller, less

transparent, and less well known entities, and are not subject to the same accountability requirements as, for example, listed companies.

(7) Whenever faced with less transparency, less of an industry profile, or less independent means of verification of the client entity, financial institutions should consider the FT or ML risk presented by the entity, and therefore the extent to which, in addition to the standard evidence, they should verify the identity of the principal beneficial owners, shareholders and/or controllers. It is important to know and understand any associations the entity may have with other jurisdictions (headquarters, operating facilities, branches, subsidiaries, etc) and the individuals who may influence its operations (political connections, etc). A visit to the place of business may be helpful to confirm the existence and activities of the business.

(8) Following its assessment of the FT or ML risk presented by the entity, the financial institution may decide to verify the identity of one or more of the partners/owners who have authority to operate an account or to give the financial institution instructions concerning the use or transfer of funds or assets, but might be waived for other partners/owners.

### 2.6.5 Clubs and societies

(1) Where an application is made on behalf of a club or society, financial institutions should make appropriate distinction between those that serve a limited social or regional purpose and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

(2) For many clubs and societies the FT and ML risks will be low. The following information should be obtained about the customer:

- full name of the club/society
- legal status of the club/society
- purpose of the club/society
- names of all officers

(3) The financial institution should verify the identifies of the officers who have authority to operate an account or to give the financial institution instructions concerning the use or transfer of funds or assets.

(4) Financial institutions should take appropriate steps to be reasonably satisfied that the person the financial institution is dealing with is properly authorized by the customer and is who he says he is.

(5) Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer’s identity.

*Variation from the standard*

(7) The financial institution's assessment may lead it to conclude that the FT risk is higher, and that it should require additional information on the purpose, funding and beneficiaries of the club or society. This might include seeing a copy of the constitution (or equivalent) of the club or society.

(8) Following its assessment of the FT risk presented by the club/society, the financial institution may decided to verify the identities of additional officers, and/or institute additional transaction monitoring arrangements (See MLFTG Part I, Section 2, para. 2.1.40).

### 2.6.6 Public sector bodies, governments, state-owned companies and supranationals

(1) In respect of customers which are Antiguan and Barbudan or overseas governments (or their representatives), supranational organisations, government departments, state-owned companies or local authorities, the approach to identification and verification has to be tailored to the circumstances of the customer.

(2) Financial institutions should obtain the following information about customers who are public sector bodies, government, state-owned companies and supranationals:

- Full name of the entity
- Nature and status of the entity [e.g. overseas government, treaty organisation]
- Address of the entity
- Name of the home state authority
- Names of directors (or equivalent)

(3) Financial institutions should take appropriate steps to understand the ownership of the customer, and the nature of its relationship with its home state authority.

(4) Financial institutions should take appropriate steps to be reasonably satisfied that the person the financial institution is dealing with is properly authorised by the customer and is who he says he is.

## 2.7 MONITORING CUSTOMER ACTIVITY

2.7.1 Section 3(1)(b) of the MLPR requires a financial institution to have "such other procedures of internal control and communication as may be appropriate for the purposes of forestalling and preventing money laundering [related to FT]"

2.7.2 There is an expectation that where the situation so warrants a financial institution will establish and maintain an appropriate approach to enable it to detect transactions or activity that may indicate terrorist financing or related money laundering.

2.7.3 In addition to carrying out customer due diligence, a financial institution may need to monitor customer activity to identify, during the course of a continuing relationship, unusual activity. Unusual activity that cannot be rationally explained may involve terrorist financing or related money laundering.

2.7.4 The essentials of any system of monitoring are that:

- It flags up transactions or activities for further examination;
- Such reports are reviewed promptly by the appropriate person;
- Appropriate action is taken on the findings of any further examination.

Monitoring can be either;

- in real time, or
- after the event

and in either case, unusual transactions or activities will be flagged for further examination.

2.7.5 Monitoring may be by reference to specific types of transactions, to the profile of the customer, or by comparing their activity or profile with that of a similar or peer group of customers, or through a combination of these approaches.

2.7.6 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the financial institution's activities and whether it is large or small.

2.7.7 Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- the usual nature of a transaction, for example, abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;
- the nature of a series of transactions: for example, a number of cash credits;
- the geographic destination or origin of a payment, for example, to or from a high-risk country;
- the parties concerned, for example, a request to make a payment to or from a person on a sanctions list.

# Chapter III —RECORD KEEPING

*This guidance is incomplete on its own — It must be read together with Section 3 of Part I of the MLFTG on money laundering and the updates thereto.*

*This chapter provides guidance on records that must be kept and how they should be preserved and produced when required.*

**Legal framework**
**Acts**
MLPA sections12, 12A, 12B
**Regulations**
MLPR Regulation 3(i)(ii), 5
**Guidelines**
MLFTG Part I, Section 3

---

**Core obligations**

- Retain copies of the Attorney General's order Declaring a Specified Entity
- Retain copies of directives to freeze property of a Specified Entity
- Retain copies of the results of database searches for customers who might be Specified Entities or transactions that might be related to Specified Entities
- Retain copies of decisions and instructions to freeze and unfreeze property relating to the Attorney General's Declaration of a Specified Entity
- Retain copies of all reports of Terrorist Property and suspicious activity related to Specified Entities and related documents
- Retain records of research on persons suspected of being financiers of terrorism

- Retain the documents collected as verification of a customer's identity for 6 years after the end of the customer relationship
- Keep a copy of the documents collected as verification of a customer's identity if it becomes necessary to surrender the original for 6 years after the end of the customer relationship
- Retain records of customer transactions for 6 years after the transaction is completed
- Retain correspondence related to customer account and customer transactions

- Retain details of action taken in respect of internal suspicious activity reports
- Retain details of action taken in respect of suspicious activity reports made to the Supervisory Authority or the Director of ONDCP

- Retain details of research done by the compliance officer in respect of an internal SAR that does not result in an external SAR, together with details of the reasons why there was no external SAR.

---

**Actions required or required to be kept under regular review**

- Maintain appropriate systems for retaining and preserving records
- Maintain appropriate systems to ensure records are legible whenever required to be produced
- Maintain appropriate systems for making records available when required by law enforcement, within the specified time period

---

### 3.1 General legal and regulatory requirements

[See MLPR regulation 5; MLFTG Part I, Section 3]

3.1.1What records must be kept

[See MLPA section 12, 12B; MLPR regulation 5]

3.1.2 Form in which records must be kept

[See MLFTG Part I, section 3; MLPR regulation 5]

### 3.2 Records relating to specified entities

3.2.1 Financial institutions should keep the originals or copies of records relevant to compliance with their obligations under the Prevention of Terrorism Act.

3.2.2 The following records should be kept:

(1) The Attorney General's order Declarating a Specified Entity;

(2) The Notice of the Attorney General's Declaration of a Specified Entity;

(3) Any directive of the Attorney General contained in the Declaration or otherwise relating to a Specified Entity, including a directive to freeze accounts and assets of the Specified Entity;

(4) Checks made of the customer database of the financial institution to determine whether accounts are held on behalf of a Specified Entity or transactions were done relating to a Specified Entity. These should include (a) the date of the first check (b) the dates of subsequent checks (c) the name and position of the staff member performing the check (d) the conclusion drawn from the check;

(5) Details of the internal decision to freeze accounts or assets of a Specified Entity in response to the Attorney General's Declaration of a Specified Entity. This should include but not limited to (a) the name and position of the person who gives the instruction to freeze, and (b) other details relevant to recording the time of freezing, the property frozen and how the property was subsequently dealt with

(c) whether the property was subsequently forfeited, or (d) the fact and basis for subsequent unfreezing the property.

(6) Reports to the Attorney General of the freezing of property of a Specified Entity;

(7) Reports to the Director of ONDCP of the possession and/or freezing of property of a Specified Entity;

(8) Any communication from the Director of ONDCP relating to a Specified Entity.

**3.3 Records relating to financiers of terrorism**

3.3.1 A list updated monthly should be kept of all persons doing business with the financial institution who are suspected of being financiers of terrorism. A record should be kept of the basis for suspecting a person of being a financier of terrorism.

3.3.2 A record and all reviews of the record should be kept of the decision with reasons as to whether or not the financial institution should continue or terminate the business relationship with a person suspected of being a financier of terrorism.

3.3.3 The records should be kept and treated as financial transaction documents as defined in the MLPA and kept for the required period, which is 6 years.

# Chapter IV — REPORTING SUSPICIOUS ACTIVITY AND POSSESSSION OF TERRORIST PROPERTY

*This guidance is incomplete on its own — It must be read together with Section 4 of Part I of the MLFTG on money laundering and the updates thereto.*

*This Chapter provides guidance on procedures financial institutions need to PUT in place so that they are able to make suspicious activity reports and terrorist property reports to the Supervisory Authority and Director of the ONDCP.*

**Legal framework**
**Acts**
PTA section 34(3), 34(4)
MLPA sections 7, 13(1A), 13(2), 13(3)
**Regulations**
MLPR regulation 3(i)(iii), 6
**Guidelines**
MLFTG Part I, Section 4

---

**Core obligations**

- All staff must make an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion that terrorist property exists
- Reports must be made on specified entities
- Reports must be made on suspected financiers of terrorism
- The Compliance Officer must consider all internal reports
- The Compliance Officer must make a report to the Director of ONDCP without delay if he/she considers that there is knowledge, suspicion or reasonable grounds for knowledge or suspicion that terrorist property exists
- Financial institutions must freeze funds in accordance with the Attorney General's directive if a customer is identified as being a specified entity and make a report to the Director of the ONDCP
- Staff must not do or say anything that might tipp off another person that an internal or external SAR has been or is about to be made or prejudice an investigation
- A suspicious activity report must be made even where a transaction is not completed or is only an attempted transaction or where there is a suspicious approach to the financial institution

---

**Actions required or required to be kept under regular review**

- Enquiries made in respect of internal suspicious activity reports must be documented

- The reasons why a suspicious activity report was, or was not submitted should be documented
- Any communications made with or received from the ONDCP in relation to a SAR or Terrorist Property Report should be kept on file

---

### 4.1 General legal requirements

[PTA section 34(3), 34(4)]
[[MLPA section 13]
[MLPR regulation 6]

### 4.2 What is to be reported

#### 4.2.1 Terrorist Property

(1) Financial institutions are required by section 34(3) of the PTA to report the **possession or control** of Terrorist Property (Property of Specified Entities).

(2) Reportable property is property belonging to, controlled by on held on behalf or for the benefit of a specified entity. That is, someone whose name, date of birth etc. matches that of a person or entity declared to be a specified entity Where the name of the person or entity was originally generated in a foreign script and then translated into the western alphabet, it may be that the name can be closely represented by two or more spellings in the western alphabet. In such instances, financial institutions should take into consideration names whose spelling are a close match or pronunciation are virtually the same. In such circumstances where all the other supporting details are a match then a report should be made, and any concern about the name not being an exact match drawn to the attention of the Director of ONDCP.

(3) The property and funds of terrorists are defined by the PTA as follows:

> **property:** assets of every kind, whether corporeal or incorporeal, moveable of immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.
>
> **funds:** means assets of every kind, whether tangible or intangible, moveable or immoveable however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including but not limited to bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

#### 4.2.2 Suspicious Activity

(1) Financial institutions are required by section 34(4) of the PTA to report transactions, attempted transactions or proposed transactions of which there is knowledge or reasonable grounds to suspect that the transaction is—

(a) related to terrorism or the commission of a terrorist act;

(b) conducted by or on behalf of a terrorist group or a member of a terrorist group;

(c) conducted by or on behalf of a person who finances terrorism or the commission of a terrorist act.";

### 4.2.3 What is meant by knowledge and suspicion?

[MLPA section 13(5)]

(1) Having knowledge means actually knowing something to be true.

(2) Suspicion is beyond speculation and based on some foundation. Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation.

(3) A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transaction or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

(4) A member of staff, including the compliance officer, who considers a transaction or activity to be suspicious, would not necessarily be expected to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing. However, where the compliance officer can identify or does have a suspicion of a criminal predicate offence, or is able to compare the suspicious activity to known criminal patterns of activity, this can be brought out in the report, particularly in Part F of the standardized Terrorist Property Report Form or Part C of the standardized SAR Form which provides for explicit indication of suspicion of *terrorist financing*.

### 4.2.4 What is meant by reasonable grounds to suspect?

[PTA section 34(6)]
[MLPA section 13(5)]

(1) Section 34(6) of the PTA introduces criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a transaction relates to terrorism or the financing terrorism. *Reasonable grounds* is determined by an objective test. Section 2(2) of the PTA provides:

> *"Knowledge, intent or purpose required as an element of any offence under this Act, as well as the relationship of any proceeds or instrumentalities to a terrorist activity, may be inferred from objective or factual circumstances."*

(2) It should also be noted that transactions conducted with the proceeds of financing of terrorism offences constitute money laundering, and as such, section 13(2A) of the MLPA applies. That section states:

> *"The question whether a reasonable suspicion for the purpose of subsection*

*(2) should have been formed, shall be determined objectively, having regard to all the facts and surrounding circumstances."*

The test would likely be met when there are demonstrated to be facts or circumstances, known to the member of staff, from which a reasonable person engaged in such business would have inferred knowledge, or formed the suspicion that another person was engaged in terrorist financing offences. Therefore, staff of a financial institution should be able to demonstrate that they took reasonable steps in the particular circumstances, in the context of a risk-based approach, to know the customer and the rationale for the transaction, activity or instruction.

### 4.3 Internal reporting

An obligation to report up the chain of supervision to the compliance officer in the financial institution where there is grounds for knowledge or suspicion of money laundering or terrorist financing is placed on all relevant employees. All financial institutions therefore need to ensure that all relevant employees know who they should report suspicions to. The reporting chain to the compliance officer should be as short as practicable.

### 4.4 Evaluation and determination by the compliance officer

The financial institution's compliance officer must consider each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. The financial institution must permit the compliance officer to have access to any information, including KYC information, in the financial institution's possession which could be relevant. The compliance officer may also require further information to be obtained, from the customer if necessary, or from an intermediary who introduced the customer in the financial institution, to the extent that the introducer still holds the information. Any approach to the customer or to the intermediary should be made sensitively, and probably by someone other than the compliance officer, to minimize the risk of alerting the customer or an intermediary that a disclosure may be under consideration.

### 4.5 External reporting (to the Director of ONDCP)

Suspicious activity reports should be made to the Director of ONDCP either by delivering a hard copy of the SAR by hand, mail or fax to:

**ONDCP Headquarters,**
**P.O. Box W827**
**Camp Blizard,**
**Antigua and Barbuda**

**Fax no.: 268 460-8818**
**Telephone no.: 268 562-3255**

SARs should be filed on the standardized reporting form — Terrorist Property Report obtainable from the ONDCP by email or the ONDCP website at www.ondcp.gov.ag. For details on preparing reports on financing of terrorism

See: **Handbook for Preparing Reports of Suspicious Activity, Significant Payments and Property of Specified Entities.**

### 4.6 Tipping off and prejudicing an investigation

[See MLPA section 7]

Once an internal or external suspicious activity report has been made in relation to the proceeds of crime (which includes proceeds of the financing of terrorism), it is a criminal offence under section 7 of the MLPA for anyone to release information which is likely to prejudice an investigation.

### 4.7 Transactions following a disclosure

(1) Transactions with property following the discovery of property of a specified entity is prohibited in accordance with a directive from the Attorney General.

(2) Section 3(2)(b) of the Prevention of Terrorism Act provides:

> "If the Attorney General is satisfied that there is material to support a recommendation made under subsection (1) [that a person be declared a specified entity], he may, by order— …
>
> (b) direct any financial institution in Antigua and Barbuda to restrain or freeze any account or other property held by the financial institution on behalf of the specified entity."

(3) Transactions following the reporting of a suspicious transaction that may be related to terrorism may for money laundering purposes become subject to further directive of the Supervisory Authority or an administrative freeze order or court order.

### 4.8 HANDLING TERRORISM-RELATED PROPERTY

STEP 1: ENSURE THAT INFORMATION HELD ON DECLARED TERRORISTS IS CURRENT

(1) Take note of Persons and Entities Designated as Terrorists by consulting the following sources:

**(a) The Attorney General's Declarations**

The Attorney General, being satisfied that a person is a terrorist, terrorist organization or person affiliated with a terrorist organization may by Order declare the person to be a specified entity.

**(b) The ONDCP Website**

Lists of Persons and Entities declared to be specified entities is available on the ONDCP website www.ondcp.gov.ag.

**(c) Other lists:**

Financial institutions may also choose to consult lists of terrorists published by other countries, such as:

- the OFAC List put out by the United States, or
- lists published by commercial concerns.

**NOTE CAREFULLY: These lists are not the basis for determining whether a person is a specified entity. The Declaration of Specified Entities by the Attorney General is the basis for treating a customer as a specified entity.**

"Other lists" show persons and entities who have been designated as money launderers or affiliates of terrorist groups so considered by other countries. This may serve to indicate persons and entities which a financial institution may consider subjecting to enhanced due diligence, and would want to carefully assess whether to do business with, or continue to do business with. The Attorney General's declaration determines who are specified entities; with these entities a financial institution has no option and must not conduct transactions.

(2) Take Note of the official means of communicating binding Notice of specified entities (sections 2A, 2B and 2C of the Prevention of Terrorism Act (as amended by section 4 of the Prevention of Terrorism (Amendment) Act 2010 )).

The PTA provides:

> (2A) For the purposes of subsection (2)(b), the Order by the Attorney General directing a financial institution to restrain or freeze any account or other property held by the financial institution on behalf of the specified entity shall be immediately binding and effective on the financial institution notwithstanding that the Order has not yet been published in the Gazette.
>
> (2B) An Order to a financial institution under subsection (2)(b) may be communicated by the Attorney General using such methods as may be appropriate in the circumstances or as may be prescribed by Regulations.
>
> (2C) Without limiting the generality of subsection (2B) the Order may be communicated by the Attorney General through the Director of the ONDCP.

(3) The Attorney General can communicate legally binding notice to a financial institution of the declaration of a specified entity by sending it a Notice of Declaration of Specified Entity. For an example of this, see Appendix 1, Form 1.

**(4) <u>Note Carefully</u>: notwithstanding the requirement for the Attorney General's Order to be gazetted, section 2A of the PTA provides for notice of the order to be immediately binding on a financial institution without production of a gazetted copy of the order. Compliance officers should be fully aware of this provision and ensure that other relevant members of staff likely to have to act in the absence of the compliance officer are also aware of the legal requirement.**

(5) The Director of the ONDCP is also authorized to officially communicate legally binding notice of the Attorney General's Declaration of Specified Entities by section 2C of the PTA, which includes by fax transmission see Appendix 1. Form 2.

STEP 2: FREEZE WITHOUT DELAY PROPERTY OWNED BY OR HELD ON BEHALF OF A SPECIFIED ENTITY

Where the Attorney General in his Declaration of a Specified Entity encloses a directive to freeze property held on behalf of a specified entity or by other means communicates such a directive, the financial institution should freeze property of the specified entity without delay and contact the ONDCP for further instructions. Financial institutions must not entertain the option of returning funds, for example, a wire transfer, that are discovered to be related to a specified entity. This may be a convenient way of avoiding involvement in the matter but is contrary to the requirement of the law which is that the property be frozen without delay.

STEP 3: IMPLEMENT THE DIRECTIVES CONTAINED IN THE ATTORNEY GENERAL'S DECLARATION OF A SPECIFIED ENTITY

**Act on the Directives contained in the Notice of the Declaration of a Specified Entity**

Upon receipt of a Notice of Declaration of a Specified Entity a financial institution should:

(1) Check its customer database to determine whether the name of any Specified Entity listed matches that of any of its customers. If so,

(2) Freeze any account or other property held by the financial institution for or on behalf of the Specified Entity, and forthwith

(3) Make a Specified Entity Property Report (Terrorist Property Report) to the Director of the ONDCP;

(4) Implement any other Directives that the Attorney General may have included in the Declaration;

(5) Make a Suspicious Activity Report of any customer suspected of being affiliated with transactions of a Specified Entity.

STEP 4: MAKE ALL REQUIRED REPORTS TO THE AUTHORITIES

**I. Terrorist Property Reports**

**(a) When accounts, funds or property in the possession or control of a financial institution are found to be held by or on behalf of a specified entity (a declared terrorist), a Terrorist Property Report (also called a Specified Entity Property Report) should be made to the ONDCP. It is good practice to speak directly to the Director of the ONDCP to inform him of the development and follow that up with the submission of the written Terrorist Property Report.**

(b) Where a financial institution is satisfied it possesses or controls property of a Specified Entity where the name of the person or entity is a close but not exact match then a Terrorist Property Report should be made to the ONDCP. It is good practice to speak directly to the Director of the ONDCP to inform him of the development and follow that up with the submission of the written Terrorist Property Report.

## II. Suspicious Activity Reports (SAR)

(a) When a transaction is suspected of being related to a specified entity, then a suspicious activity report should be made to the ONDCP pursuant to section 34 of the PTA;

(b) When a transaction is suspected of being related to terrorism (even if a specified entity is not identified as being involved) then a suspicious activity report should be made to the ONDCP. Circumstances surrounding a transaction(s) can raise questions about a relationship to terrorism without a specified entity being identified, for example, funds remitted regularly to certain high risk jurisdictions without a satisfactory explanation or where there is no natural connection or economic sense of the transaction(s).

(c) When a transaction is suspected of being related to a financier of terrorism or someone suspected of being a financier of terrorism, then a suspicious activity report should be made to the Director of the ONDCP;

### How to file a report

Reports should be made on the appropriate standardized reporting forms which elicit critical information on the activity being reported. These forms are available from the ONDCP by email or from the ONDCP website at www.ondcp.gov.ag. Detailed guidance on how to fill out the forms, particularly in response to those queries that are somewhat unintuitive is available in the **"Handbook for Preparing Reports of Suspicious Activity, Significant Payments and Terrorist Property"** which is issued by the Supervisory Authority to supplement the MLFTG. This is available from the ONDCP by email or from the ONDCP website at www.ondcp.gov.ag.

STEP 5: TAKE NOTE OF ANY ANCILLARY DIRECTIVES FROM THE DIRECTOR OF ONDCP

### Responding to Any Directives of the Director of ONDCP

A Declaration of Specified Entity will contain a number of Directives from the Attorney General with which a financial institution must comply. There are two types of directive: (1) the standard directives which will be included with all Notices of Declaration of Specified Entity, and (2) any other directive the Attorney General considers necessary for the financial institution to properly respond to the declaration. (See Step 3 above.) However, there may be other things that need to be done depending on the circumstances and contingencies. Instructions related to this may be received from the Director of the ONDCP.

STEP 6: REMOVE FROM CFT MONITORING THE NAMES OF PERSONS WHO ARE NO LONGER LISTED AS SPECIFIED ENTITIES

### De-Listing Specified Entities

In addition to his powers to declare persons to be Specified Entities, the Attorney General has a duty to give notice when persons have been removed from the list of specified entities because they are no longer considered to be terrorists or terrorist affiliates.

The Attorney General after making a decision to de-list specified entities will send to all financial institutions a Notice of De-Listing of Specified Entity. For an example of this see Appendix 1, Form 3

# Chapter V — STAFF AWARENESS, TRAINING AND ALERTNESS

*This guidance is incomplete on its own — It must be read together with Section 5 of Part I of the MLFTG on money laundering and the updates thereto.*

*This chapter provides guidance on training of staff to ensure that as the frontline implementers of a financial institution's AML/CFT policies and controls they understand what is required of them and are able to carry out their functions competently.*

**Legal framework**
**Acts**
MLPA section 11(viii)
**Regulations**
MLPR regulation 3(1)(c)
**Guidelines**
MLFTG Part I, Section 5

---

**Core obligations**

- Relevant employees should be
    - Made aware of terrorist financing, the relevant legislation, and their obligations under that legislation
    - Made aware of the identity and responsibility of the compliance officer of the financial institution
    - Trained in relevant procedures and how to recognize and deal with potential money laundering and financing of terrorism transactions or activity
- Staff training should be given at regular intervals and details recorded
- Compliance officer is responsible for oversight of compliance with AML/CFT requirements in respect of staff training
- The relevant director or senior management should have overall responsibility for the establishment and maintenance of effective training arrangements

---

**Actions required or required to be kept under regular review**

- Provide appropriate training to make relevant employees aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the financial institution
- Ensure that relevant employees are provided with information on, and understand, the legal responsibilities and liabilities of the financial institution and individual members of staff and of changes to these legal positions
- Consider providing relevant employees with case studies or examples related to the business of the financial institution

- Train relevant employees in how to operate a risk based approach to CFT

---

**5.1 Reason for staff awareness and training**

One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of ML and FT and well trained in the identification of unusual activities or transactions which may prove to be suspicious. The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the financial institution's AML/CFT strategy.

In is essential that financial institutions implement a clear and well articulated policy for ensuring that relevant employees are aware of their obligations in respect of the prevention of ML and FT and training them in the identification and reporting of anything that gives grounds for suspicion. This is especially important for staff who handle customer transactions or instructions. Temporary and contract staff carrying out such functions should also be covered by these training programs.

Under the MLPA and MLPR individual members of staff face criminal penalties if they are involved in money laundering, FT-related money laundering, or if they do not report their knowledge or suspicion of ML or FT where there are reasonable grounds for their knowing or suspecting such activity. It is important, therefore, that staff are made aware of these obligations, and are given training in how to discharge them.

**5.2 General legal and regulatory obligations**

A financial institution's commitment to training and competence are that:

- its employees are competent;
- its employees remain competent for the work they do;
- its employees are appropriately supervised;
- its employees' competence is regularly reviewed;
- the level of competence is appropriate to the nature of the business.

**5.3 Responsibilities of financial institution and its staff**

Relevant employees should be trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions will need different training, tailored to their particular function.

Sufficient training will need to be given to all employees to enable them to recognise when a transaction is unusual or suspicious, or when they should have reasonable grounds to know or suspect that ML or FT is taking place.

The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious,

will depend on the customer and the product or service in question. Illustration of situations that may be unusual and which in certain circumstances might give rise to reasonable grounds for suspicion, are:

- transactions which have no apparent purpose, or which make no obvious economic sense (including where a person makes a loss against tax, or which involve apparently unnecessary complexity;
- the use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
- where the transaction being requested by the customer, or the size or pattern of transactions, is, without reasonable explanation, out of the ordinary range of services normally requested or is inconsistent with the experience of the financial institution in relation to the particular customer
- dealing with customers not normally expected in that part of the business
- transfers to and from high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;
- where a series of transactions are structured just below a regulatory threshold;
- where a customer who has entered into a business relationship with the financial institution, particularly deposit taking institutions like banks and credit unions, uses the relationship for a single transaction or for only a very short period of time.
- unnecessary routing of funds through third party accounts;
- unusual investment transactions without an apparently discernible profitable motive.

Issues relating to the customer identification process that may raise concerns include such matters as the following:

- Has the customer refused, or appeared particularly reluctant, to provide the information requested without reasonable explanation?
- Do you understand the legal and corporate structure of the client entity, and its ownership and control, and does the structure appear to make sense?
- Is the staff member aware of any inconsistencies between locations and other information provided?
- Is the area of residence given consistent with other profile details, such as employment?
- Does an address appear vague or unusual - e.g., an accommodation agency, a professional 'registered' office' or a trading address?
- Does it make sense for the customer to be opening the account or relationship in the jurisdiction that he is asking for?

- Is the information that the customer has provided consistent with the banking or other services or facilities that he is seeking?
- Does the supporting documentation add validity to the other information provided by the customer?
- Does the customer have other banking or financial relationships with the financial institution, and does the collected information on all these relationships appear consistent?
- Does the client want to conclude an arrangement unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained?
- Has the customer suggested changes to a proposed arrangement in order to avoid providing certain information?

Staff should also be on the lookout for such things as:

- sudden, substantial increase in cash deposits or levels of investment, without adequate explanation.
- transactions made through other banks or financial institutions;
- regular large, or unexplained, transfers to and from countries known for money laundering, terrorism, corruption or drug trafficking;
- large numbers of electronic transfers into and out of the account;
- significant/unusual/inconsistent deposits by third parties; and reactivation of dormant account(s).

**Examples of activity that might suggest to staff that there could be potential terrorist activity include:**

- **round sum deposits, followed by like-amount wire transfers;**
- **frequent international ATM activity;**
- **no known source of income;**
- **use of wire transfers and the internet to move funds to and from high-risk countries and geographic locations;**
- **frequent address changes;**
- **purchases of military items or technology; and**
- **media reports on suspected, arrested terrorists or groups.**

**5.4 Training methods and assessment**

Whatever the approach to training, it is vital to establish comprehensive records to monitor who has been trained, when they received the training, the nature of the training given and its effectiveness.

| **Abbreviations used in Part II of the ML/FT Guidelines** | |
|---|---|
| AML | anti-money laundering |
| CFT | counter financing of terrorism |
| ID | identification |
| KYC | know your customer |
| ML | money laundering |
| FATF | Financial Action Task Force |
| FT | financing of terrorism |
| MLFTG | Money Laundering and Financing of Terrorism Guidelines |
| MLPA | Money Laundering (Prevention) Act 1996, as amended |
| Para. | paragraph |
| PTA | Prevention of Terrorism Act 2005 |
| SAR | Suspicious Activity Report |
| SR | Special Recommendation of the FATF |

# APPENDICIES

## APPENDIX 1 — FORMS

1. Notice of Declaration of Specified Entity
2. Fax Notice of Specified Entity from the Director of ONDCP
3. Notice of De-listing of Specified Entity
4. Other relevant Forms: See the Handbook for Reporting Suspicious Activity, Significant Payments and Terrorist Property

## APPENDIX II — SUMMARY OF FINANCING OF FINANCING OF TERRORISM LAW

# APPENDIX I: FORMS

# NOTICE OF DECLARATION OF SPECIFIED ENTITY

(Section 3(2) of the Prevention of Terrorism Act 2005)

**TO: FINANCIAL INSTITUTIONS under the Prevention of Terrorism Act 2005.**

**TAKE NOTICE** that the ATTORNEY GENERAL under section 3(2) of the Prevention of Terrorism Act 2005 has by Order dated the …… day of …….., 20…… declared the following listed person(s) to be Specified Entities:

- ……..
- ……..
- ……..

**AND TAKE NOTICE** that the Order of the Attorney General takes immediate effect.

**THAT** pursuant to section 2A of the Prevention of Terrorism Act 2005 as amended the Order of the Attorney General is immediately binding and effective on all financial institutions notwithstanding that a *gazetted* copy of the order may not accompany the Notice.

**In Consequence** the ATTORNEY GENERAL pursuant to section 3(2)(b) of the Act has Directed as follows—

**DIRECTIVE to Financial Institutions:** A Financial Institution to whom this notice is communicated shall without delay: (1) Check its customer database to determine whether the name of any Specified Entity listed above matches that of any of its customers. If so, (2) Freeze any account or other property held by the financial institution for or on behalf of the Specified Entity, and forthwith (3) Make a Specified Entity Property Report to the Director of the ONDCP, etc.

**"Freeze" means that the account or other property or such part of it as specified by Directive is not to be disposed of or otherwise dealt with by any person except in such manner and in such circumstances as are specified in the Directive or subsequent Order of a Court as provided by the Act.**

Signed:

Attorney General

# OFFICE OF NATIONAL DRUG AND MONEY LAUNDERING CONTROL POLICY (ONDCP)

# FAX

To:

From: **The Supervisory Authority, Money Laundering (Prevention) Act 1996**

Fax: Pages:

Phone: Date:

Fax: Phone:

Re: **NOTICE OF DECLARATION OF SPECIFIED ENTITY**

Urgent [✓] For Review [] Please Comment [] Please Reply [] Confidential [✓]

The information contained in this Facsimile message is privileged, confidential and exempt from disclosure under applicable law. It is intended only for the use of the individual or entity to which it is addressed above and others who have been specifically authorized to receive it. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone to arrange for return of the original documents to us. Thank you.

**URGENT:** Attached for your immediate attention and action is a Notice of the Attorney General's Declaration of Specified Entities made by Order on the day of 20___ . You are required to read the Notice and implement any Directives contained therein.

THE DIRECTOR OF THE ONDCP is authorized by section 2C of the Prevention of Terrorism Act 2005 as amended to communicate the DECLARATION OF SPECIFIED ENTITIES and THE DIRECTIVE to Financial Institutions with legally binding effect. The Director of the ONDCP may communicate this Notice by usual means that may include facsimile transmission and email or as prescribed by regulation.

Signed: Director, ONDCP

# NOTICE OF DELISTING OF SPECIFIED ENTITY

(Section 5A of the Prevention of Terrorism Act 2005)

**TO: FINANCIAL INSTITUTIONS under the Prevention of Terrorism Act 2005.**

TAKE NOTICE that the ATTORNEY GENERAL pursuant to section 5A(a) of the Prevention of Terrorism Act 2005 has revoked the Declaration Order of Specified Entities dated the …… day of ……., 20…… with respect to the following persons or entities:

- ……..
- ……..
- ……..

AND TAKE NOTICE that the Order of the Attorney General takes immediate effect.

Financial Institutions receiving this notice should discontinue enhanced due diligence procedures put into effect specifically in response to the Declaration Order that has now been revoked.

Properties delisted person(s) or entities which were frozen by Court Order should be dealt with in accordance with a further Court Order when received unfreezing the property.

Signed:

Attorney General and
Minister of Legal Affairs

# APPENDIX II: Summary of Financing of Terrorism Law

## The Prevention of Terrorism Act 2005

Relevant law and guidance include the following:

- **Prevention of Terrorism Act 2005**
- **Prevention of Terrorism (Amendment) Act 2008**
- **Prevention of Terrorism (Amendment) Act 2010**
- **United Nations 1267 Committee Consolidated List of Terrorist Persons and Entities**
- **Supplemental Guidelines on Annual Audit Reports and Audit Reviews**
- **Handbook for Preparing Reports on Suspicious Activity, Significant Payments and Terrorist Property**

Key definitions for understanding the obligations of financial institutions.

**"financing of terrorism"** includes, without limiting the generality, such conduct as is prohibited by sections 6, 7, 8, 9 and 10 of the Prevention of Terrorism Act 2005

**funds:** means assets of every kind, whether tangible or intangible, moveable or immoveable however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including but not limited to bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

**property:** assets of every kind, whether corporeal or incorporeal, moveable of immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.

# PART III — SECTOR SPECIFIC GUIDELINES

## SECTOR SPECIFIC GUIDELINES
## MONEY TRANSMISSION SERVICES

*This guidance is incomplete on its own — It should be read together with Parts I and II of the MLFTG on money laundering and the updates thereto and on the financing of terrorism.*

1. All customers of a money value transmission service must be identified, irrespective of the threshold of the transaction involved. Minimum identification should include:

(1) name
(2) address
(3) date of birth
(4) citizenship

2. A person who is registered as a money transmission service should keep a record of all agents and subagents of the business. That record should be kept current.