MONEY LAUNDERING & THE FINANCING OF TERRORISM

GUIDELINES FOR FINANCIAL INSTITUTIONS*

UPDATE

[AMENDMENT ISSUED January 2004]

The Supervisory Authority for Money Laundering and the Financing of Terrorism†
O.N.D.C.P. Headquarters
Camp Blizard
Coolidge
Antigua, West Indies
Telephone: 562-3255, (268) 462-5934
Fax: (268) 460-8818
email: ondcp@candw.ag

---

* Section 11(vii) of the Money Laundering (Prevention) Act 1996 & Regulation 2 of the Prevention of Terrorism Regulations 2004
† Section 10 of the Money Laundering (Prevention) Act 1996 & Section 2 of the Prevention of Terrorism Act 2001

NOTICE OF AMENDMENT

To all Financial Institutions: Take notice that the Money Laundering Guidelines for Financial Institutions are amended as follows:

1. The name of the guidelines is hereby changed from "Money Laundering Guidelines for Financial Institutions" to "Money Laundering & The Financing of Terrorism Guidelines for Financial Institutions".

2. The heading to the Introduction to the Guidelines is amended to insert after the word "LAUNDERING" the words "& THE FINANCING OF TERRORISM"

3. At the end of the Introduction to the Guidelines the following is inserted:

   "THE FINANCING OF TERRORISM

   The UN International Convention for the Suppression of Terrorism defines terrorism as an "Act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act." The financing of terrorism could be described as the contribution to, collection or retention of funds with the knowledge that they will be or are likely to be applied to the bringing about of a terrorist act.

   [Appendix B to these Guidelines contains a summary of the Antigua and Barbuda legislation on the financing of terrorism]"

4. Paragraph 1.0 is amended after the sentence, "Institutions must therefore appoint a Compliance Officer to undertake this role", by inserting the following sentence: "In order to be in a position to effectively fulfil the functions and demands of that role, the Compliance Officer should be appointed at management level."

5. The following Paragraph is inserted after Paragraph 1.1:

   "1.1A Financial institutions should put in place adequate screening procedures to ensure high standards when hiring employees. This can include obtaining proper documents of identification, references, and where appropriate police records and interviewing past employers.

6. The following paragraphs are inserted after Paragraph 1.3:

"1.3A Financial institutions that were issued Supervisory Authority Directive No. 1 of 2003, which includes all banks, should, as stated in the directive, instruct their internal and external auditors to review their anti-money laundering (and combating financing of terrorism) systems and submit a separate annual anti-money laundering/combating the financing of terrorism audit report (Annual AML/CFT Audit Report) to the Supervisory Authority in September of each year. The audit should be an assessment of (1) the extent to which the required AML/CFT policies, controls and procedures are in place, and (2) the extent to which the AML/CFT system is functioning effectively. The report should as a minimum contain the following information:

1. Brief description of the activities and services offered by the bank

2. Description of the procedures used to review the bank's AML/CFT system. (Note: the procedures should include devised tests of the AML/CFT system (these may be simple or sophisticated as long as they properly measure the effectiveness with which the system functions, e.g. testing whether a teller requests source of funds information of a customer at an appropriate point, or whether an employee makes a suspicious transaction report to the compliance officer where an applicant for business terminates an application when asked required questions, etc.). Elements of the system should be routinely subjected to random tests without prior warning to staff.).

3. .Description of the AML/CFT system, including:

   Internal controls and procedures

   Identification procedures (due diligence)

   Record Keeping

   Recognition and reporting of suspicious transactions

   Vigilance for terrorism financing

   Education and training

4. Results of tests of effectiveness conducted on the system

5. Final evaluation."

"1.3B The supervision of international banking can only be effectively carried out on a consolidated basis, and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally.

7. The following paragraphs is inserted after Paragraph 1.4:

"1.5 Financial Institutions should ensure that the principles mentioned above are also applied to their branches and subsidiaries abroad, especially in countries which do not or insufficiently apply these recommendations, to the extent that the local applicable laws and regulations permit. Financial Institutions should inform the Regulator and the Supervisory Authority when the local applicable laws and regulations prohibit the implementation of these guidelines."

"Insurance Business

1.6 Insurers and insurance intermediaries should adopt and enforce anti money laundering and terrorism financing policies, procedures and controls that will govern their activities. They also need to ensure that their internal control systems are such as to ensure that policies adopted by their boards and management for preventing and deterring money laundering and the financing of terrorism are fully implemented, and that prompt follow-up action, such as reporting suspicious transactions to the Supervisory Authority is taken.

1.7 Financial institutions registered or authorized to carry on insurance business under the amended International Business Corporations Act, Cap. 222 of the 1992 revised laws of Antigua and Barbuda should comply with the provisions of the Guidelines for International Insurance Corporations on Anti-Money Laundering and Combating the Financing of Terrorism (GIIC) issued in December 2003 by the Financial Services Regulatory Commission. Matters not specifically addressed in those Guidelines should be dealt with using the provisions of these Guidelines issued by the Supervisory Authority.

1.8 Financial institutions registered or authorized to carry on insurance business under the Insurance Act, Cap. 5 of the 1992 revised laws of Antigua and Barbuda should be guided by these Guidelines issued by the Supervisory Authority generally, and in addition, can look to the offshore guidelines, GIIC issued by the FSRC as a best

practices guide, and should follow the GIIC guidance set out in Paragraphs 10 to 28 — Customer Identification, and Basic Principles and Policies of Insurance Entities, Paragraphs 36, 62 to 66 — Verification and specific activities, and Paragraphs 75 to 78— Keeping of Records, until a complete set of guidelines for domestic insurance companies are issued by the end of February 2004.

1.9 Most important among these guidelines are the ones concerning internal controls. That being considered, **it must be carefully noted that the experience with international assessments made using the Core Principles set out by the International Association of Insurance Supervisors (IAIS) on which the GIIC has been based, has revealed that in many cases internal control procedures within insurance entities are not well established and supervisors have been weak in promoting their development. If management and supervisors are not able to rely on internal control systems for general operating purposes, it will be unlikely that company management and staff will have effective anti money laundering and terrorism financing controls.**

"Financing of Terrorism

"The Prevention of Terrorism Act 2001 is designed to enable law enforcement authorities in Antigua and Barbuda as part of a coordinated international effort, to identify, disrupt and dismantle terrorist financing networks. It does this by providing law enforcement with powers to freeze the assets of designated terrorists or terrorist organisations, by requiring financial institutions to maintain possession and control of any terrorist related assets discovered to be in their possession or control, and requiring them to report the fact of being in possession or control to the proper authority. Financial institutions should put in place a procedure for responding to notification by the authority of persons designated as terrorists or terrorist organizations, or for reporting that fact to the authority on becoming aware of being in possession or control of funds or property of terrorists or terrorist organizations.

"Authorities

I. The competent authority responsible under the law for administering the provisions of the Prevention of Terrorism Act 2001 is the Supervisory Authority. This is the same person designated as such under Section 10 of the Money Laundering (Prevention) Act 2001. The Supervisory Authority's office is at ONDCP Headquarters, Camp Blizard, Coolidge, Antigua. Telephone: 562-3255.

II. Financial institutions should be aware that the Supervisory Authority has the power under Section 3(4) of the Prevention of Terrorism Act 2001 to impose an administrative freeze on the funds and property of anyone designated a terrorist or entity designated a terrorist organization. This power to freeze assets is exercised by written direction to a financial institution and stays in force for 3 months unless revoked by the Supervisory Authority or by the High Court.

III. Upon receiving notification of the written direction of the Supervisory Authority to freeze assets of a designated terrorist, a financial institution should do so without delay. The phrase *without delay* means, ideally within a matter of hours of receipt of the notification from the Supervisory Authority."

8. The following paragraphs are inserted after Paragraph 2.1.4:

"2.1.4A Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalised investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted. They must, for example, be open to review by compliance officers and auditors.

"2.1.4B If a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced due diligence procedures to the customer. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities.

"2.1.4C A financial institutions should not accept or maintain a business relationship if it knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the financial institution may have under criminal law or other laws or regulations.

9. The following Paragraph is inserted after Paragraph 2.1.5:

"Customer acceptance policy

2.1.5A Financial institutions should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to the institution. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. **On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons, should be taken exclusively at senior management level."**

Politically exposed person (PEP): Business relationships with individuals holding important public positions or entrusted with prominent public functions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. A financial institution needs to bear in mind that such public positions carry with them inherently the potential or opportunity for abuse through the misuse or misappropriation of public funds or the illicit acceptance of private funds. PEPs include heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.

"2.1.5B Banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. It should also seek to identify those persons, companies and legal entities that are related to a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to

open an account for a PEP should be taken at a senior management level.

"2.1.5C There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer. Such indicators can include the country of origin and source of funds, the type of transactions involved, and other risk factors."

10. The following Paragraph should be inserted after Paragraph 2.1.7:

"2.1.7A At the time of establishing a business relationship and throughout the course of that relationship a financial institution should make itself aware of:

- the person or entity that maintains an account
- those on whose behalf an account is maintained (the beneficial owners)
- the beneficiaries of transactions conducted by professional intermediaries;
- any person or entity connected with the account or a financial transaction who can pose a significant reputational or other risk to the bank.
- whether a customer is a PEP.

11. The following paragraph is inserted after Paragraph 2.1.16:

"2.1.16A Satisfactory evidence of identity for natural persons includes one or a combination of more than one identification documents issued by a government or government authority, which indicates the person's name, date of birth, residential address, and country of citizenship, and bears a photograph of the person. Such documents include:

- valid passport
- voter registration card
- national identity card
- driving licence

2.1.16B Documents which are easily obtained in any name should not be accepted uncritically. Examples include:

- birth certificate
- identity card issued by an employer
- credit card
- business card
- national health or insurance card
- student identification card"

12. The following Paragraph is inserted after Paragraph 2.1.39:

"Unincorporated businesses and partnerships

2.1.39A In the case of accounts to be opened for unincorporated businesses, verifications of the principals in the business and all persons having authority to operate the account should be made. A copy of any business registration form or business licence should be obtained.

2.1.39B In the case of accounts to be opened for a partnership, verification of all partners of the firm who are relevant to the application and have individual authority to operate the account or otherwise to give relevant instructions should be made. Verification should proceed as if the partners were directors of a company. In the case of a limited partnership, the identity of the general partner should be verified. Changes in the composition of a partnership should be regularly monitored, and verification carried out on any new partners. Copies of the following documents should be obtained:

- partnership agreements
- for each partner, the same documents as for natural persons"

13. The following Paragraph is inserted after Paragraph 2.1.46:

"Correspondent Banking

2.1.47 Banks should have policies and procedures regarding the opening of correspondent accounts. The policy and procedures should at the minimum require the bank:

To fully understand and document the nature of the respondent bank's management and business;

To ascertain that the respondent bank has effective customer acceptance and KYC policies and is effectively supervised;

To identify and monitor the use of correspondent accounts that may be used as payable-through accounts; and

Not to enter into or continue a correspondent relationship with a bank incorporated in a jurisdiction in which it has no physical presence (i.e. meaningful mind and management) and which is unaffiliated with a regulated financial group (i.e. shell banks).

14. The following paragraph is inserted after Paragraph 3.1:

"3.1A Financial institutions, including money remitters, should include accurate and meaningful originator information on funds transfers and related messages. Originator information should remain with the transfer or related message through the payment chain. Originator information should include name, address, and account number (when being transferred from an account). In the absence of an account a unique reference number should be included or an identifier that will permit the transaction to be traced back to the originator.

15. The following paragraph is inserted after Paragraph 4.3:

4.3A Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis.

"Transactions with jurisdictions with inadequate anti money laundering systems

4.3B The FATF has listed as "non-cooperative" certain jurisdictions that have substandard or non-existent anti-money laundering/terrorist

financing legal frameworks and institutional structures. Financial institutions should make themselves aware of these jurisdictions, an updated list of which can be found at the FATF website: http://www1.oecd.org/fatf/NCCT_en.htm. Transactions from these countries should be given particular attention. Significant money laundering has been detected in this country from at least one of the states so listed in January 2004. However, the experience of Antigua and Barbuda has revealed that, relying on the *blacklisting* or even the *whitelisting* of countries may lead to complacency by financial institutions in exercising their duty of vigilance over transactions, and may actually cause a bank to lose the scent of the trail that might lead to the discovery of money laundering. The fact is that Antiguan and Barbudan financial institutions report doing a small to non-existent amount of business with most of those jurisdictions named by the FATF.

Furthermore, the fact is that 80% of all suspicious transaction reports and cases of confirmed money laundering in Antigua and Barbuda from 1996, related to transactions that originated in or passed through correspondent banks in countries that are part of the OECD/FATF and that have substantial and reputable anti-money laundering/terrorist financing systems, including not only legislation and legal measures but also implemented procedures. Actual cases indicate that substantial amounts of laundered funds have passed through correspondent accounts of reputable financial institutions in some of these countries, where, for whatever reason those institutions were unable to detect patterns of funds flow or account details that might have suggested a problem with transactions that were taking place. The Antiguan and Barbudan experience has shown that those countries with which it does the most trade and commerce and with which it has some of the closest language and cultural connections tend to be the countries from which the majority of money laundering cases has in the past originated. These countries were the United States of America, the United Kingdom, and Canada.

Financial institutions therefore, should formulate policies for dealing with foreign transactions, which define procedures that strike a functional realistic and practical balance, designed to attain as much as possible a high detection rate of suspicious transactions, without causing disruption to the normal course of business and commerce. Generally, all transactions should be looked at diligently and with care. The country of origin of a transaction should not be used as an automatic stamp of a source of legitimate funds, and is not of itself a reason to be less vigilante. Financial institutions should look to what they have learned from their due diligence and

KYC procedures, and from past experience of dealing with customers, institutions and countries. Where the financial institution is reasonably satisfied that it knows who it is dealing with that can be used to facilitate the transactions process. In other cases, KYC procedures and knowledge of financial business and its trends can provide good guidance. In all cases, financial institutions must develop through experience over time and through the methodical application of their AML/CFT policies, the sensitivity, instincts and know-how to detect and deal with suspicious transactions and activities.

To help in this procedure, deposit taking financial institutions should consider the feasibility of implementing the use of software designed to detect money laundering trends based on defined parameters."

16. The following is inserted after Paragraph 4.20:

"Detecting and reporting terrorist funds and assets

4.21 Most designated terrorists or terrorist organizations exist in foreign countries. Their designation as such is done by publication by the Supervisory Authority of their names in the Gazette, usually closely reflecting the list of terrorists published by the United Nations. In addition the Supervisory Authority will regularly circulate the names of terrorists and terrorist organizations to financial institutions. Upon publication of the names of a designated terrorist or terrorist organization in the Gazette, a financial institution should immediately make a check of its records to establish whether or not anyone so named holds an account with them. If a match is found this should be immediately communicated to the Supervisory Authority by the quickest means and transactions in the account should not proceed before contact is made and the matter discussed with the Supervisory Authority.

4.22 Financial institutions should appoint a particular person to be responsible for communicating to or being the point of contact with the Supervisory Authority on matters relating to the financing of terrorism and the provisions of the Prevention of Terrorism Act 2001. It is suggested that the financial institution's Compliance Officer for money laundering may in most cases be the appropriate person to assume this function.

4.23 If an initial report to the Supervisory Authority confirming the possession or control of funds or assets of a designated terrorist or terrorist organization is other than in writing, it should subsequently be confirmed by a written report to the Supervisory Authority"

17. Paragraph 5.1 of the Guidelines is amended by replacing the reference to "Regulation 8" with the words "Regulations 3(b) and 3(c)".

18. Appendix A is amended under the subheading "International banking/trading finance" after the fifth bullet point "Unexplained electronic fund transfers...through an account", by inserting the following bullet point:

    - Wire transfers that do not contain complete originator information

19. Appendix B is amended as follows:

    In the heading to Appendix B there is inserted after the word "LAUNDERING" the words "AND THE FINANCING OF TERRORISM".

    At the end of Appendix B the following is inserted ast a new paragraph:

    "**The Prevention of Terrorism Act 2001**

    Section 3(1) empowers the Supervisory Authority appointed under the Money Laundering (Prevention) Act 1996 to designate a person a terrorist or terrorist organisation. The names of designated terrorists or terrorist organisations are published in the Gazette.

    Section 3(4) Upon designation of a person as a terrorist or terrorist organisation, the Supervisory Authority shall issue a written direction to any financial institution in Antigua and Barbuda requiring it to restrain or freeze any account or other property held by that financial institution on behalf of that person. Such a direction from the Supervisory Authority shall have effect for three months.

    Section 5 makes it an offence to deal with property of or held on behalf of a terrorist and terrorist organisation by any person in Antigua and Barbuda.

    Section 6 makes the provision or acquisition of financial services or any other services by any person in or under the jurisdiction of Antigua and Barbuda for the benefit of or on the direction or order of any known terrorist or terrorist organisation an offence.

    Section 7 makes it an offence for any bank or financial institution in Antigua and Barbuda to transact any business with any person associated with or suspected of having any relationship with any terrorist or terrorist organisation.

Section 8 Any person who becomes aware that he has possession of or control over any funds or other assets in which a terrorist or terrorist organisation, or agent, or affiliate has an interest must retain possession and maintain control over such funds or assets, and report their existence to the Supervisory Authority.

Section 9 The Supervisory Authority is empowered for purposes of implementing the provisions of the Act and purposes relating to the prevention of terrorism, to investigate, regulate, review or prohibit any transaction in foreign exchange, or any transfer or credit or payment by, through or to any banking institution where such transfers or payments involve any interests of any foreign country or national thereof.

Section 9(3) The Supervisory Authority is empowered to request the production of any records or documents in relation to any matter in connection with any assets frozen under the Act."

Issued: 29 January 2004

.....

Wrenford D. Ferrance
Supervisory Authority under the Money Laundering (Prevention) Act 1996, and
Director, ONDCP