

**MONEY LAUNDERING &
THE FINANCING OF TERRORISM**

**GUIDELINES FOR FINANCIAL
INSTITUTIONS**

UPDATE

[AMENDMENT ISSUED 31 July 2006]

**The Supervisory Authority for Money Laundering
O.N.D.C.P. Headquarters
Camp Blizzard
Antigua, West Indies
Telephone: (268) 562-3255
Fax: (268) 460-8818
Email: supervisoryauthority@ondcp.gov.ag**

Money Laundering & The Financing of Terrorism Guidelines

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

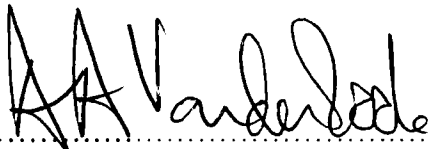
1. Paragraph 2.1.4 of the Money Laundering & Financing of Terrorism Guidelines is amended by inserting after the first sentence the words:
“Financial institutions must also obtain information on the purpose and intended nature of the business for which an account is being opened.”
2. Paragraph 2.1.5A (see the January 2004 amendment to the Guidelines) is amended by inserting after the words **“source of funds”** the words **“or source of wealth”**.
3. Paragraph 2.1.5B (see the January 2004 amendment to the Guidelines) is amended by inserting after the words **“source of funds”** the words **“or source of wealth”**.
4. Paragraph 3.1A (see the January 2004 amendment to the Guidelines) is hereby repealed and in its place, there is inserted after paragraph 3.3 new paragraphs 3.4 to 3.13 as contained in the updater page attached hereto, which should be inserted into the Guidelines after page 21 as pages 21A-1 to 21A-3.
5. The following paragraph is inserted after Paragraph 4.2 of the Guidelines:
“4.2A Financial institutions should examine as far as possible the background and purpose of suspicious transactions and make a written record of their findings.”
6. The whole of Paragraph 4.3B (see the January 2004 amendment to the Guidelines) is repealed and replace with the following:
“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 and keep updated to any changes in the listing. An updated list of such jurisdictions can be found at the FATF website: http://www1.oecd.org/fatf/NCCT_en.htm. Transactions with these countries or territories should be given particular attention.

Financial institutions should formulate policies for dealing with foreign transactions and establish

procedures that strike a functional and practical balance, designed to attain as much as possible a high detection rate of suspicious transactions (including a reasonable percentage of false positives). Generally, all transactions should be looked at diligently. The country of origin of a transaction should be noted but should not be used to automatically presume the source of funds as impliedly legitimate, or as a reason to be less than 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 satisfied from its KYC process that it has learned sufficient to satisfy itself that it knows who it is dealing with, that fact may be used to more quickly make determinations about how and at what rate a transaction should be processed. Also, knowledge of financial and business trends can provide useful indications on the nature of transactions that are being conducted. On the whole, financial institutions must develop through experience and through the methodical application of their KYC procedures, the sensitivity, instincts and know-how to detect and deal with suspicious international transactions and activities.

To help in this process, deposit taking financial institutions are encouraged to evaluate and give serious consideration to the feasibility of implementing the use of software designed to automatically detect possible money laundering trends in transactions.”

Issued: 31 July 2006



.....
Alec Vanderpoole
Supervisory Authority under the
Money Laundering (Prevention) Act 1996

UPDATER Pages — [Insert after page 21 as 21A-1 to 21A-3]

Wire Transfers

- 3.4 Wire transfers have been identified as particularly vulnerable to being used for terrorist financing and money laundering. Wire transfer and funds transfer refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person. Originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.
- 3.5 Wire transfers can be cross-border or domestic. Cross-border transfer means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element. Domestic transfer means any wire transfer where the originator and beneficiary institutions are located in the same jurisdiction. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction.
- 3.6 The licensed institutions shall take measures to include full originator information, that is, accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain. The licensed institutions shall conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

Cross-border Wire Transfers

- 3.7 Cross-border transfers should be accompanied by accurate and meaningful originator information that must at a minimum include the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included. However, the financial institutions may in their discretion substitute the address with a national identity number, customer identification number, or date and place of birth.
- 3.8 Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they shall be

Money Laundering & The Financing of Terrorism Guidelines

exempted from including full originator information, provided they include the originator's account number or unique reference number, and the batch file contains full originator information that is fully traceable within the recipient country. However, financial institutions are required to ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.

Domestic wire transfers

- 3.9 Information accompanying domestic wire transfers must also include the same originator information as indicated for cross-border wire transfers, unless the bank is satisfied that full originator information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the financial institution need only include the account number or a unique identifier provided that this number or identifier will permit the transaction to be traced back to the originator. The information must be made available by the ordering financial institution within three (3) business days of receiving the request either from the beneficiary financial institution or from appropriate authorities.

Exemptions

- 3.10 The above guidelines regarding wire transfers do not cover any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. They also do not apply to financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by these guidelines, and the necessary information should be included in the message.

Role of Ordering and Intermediary Financial Institutions

- 3.11 The ordering financial institution must ensure that qualifying wire transfers contain complete originator information. The ordering financial institution must also verify this information for accuracy and maintain this information in accordance with the requirements of the Money Laundering Act and the Prevention of Terrorism Act and any regulations issued thereunder.
- 3.12 For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.

Role of Beneficiary Financial Institution

- 3.13 Beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the Supervisory Authority. Where necessary, the beneficiary financial institution must consider restricting or even terminating its business relationship with financial institutions that fail to meet these standards.