

CARIBBEAN AML/CTF PRINCIPLES  
**ASSOCIATED GUIDELINES**

### PREAMBLE

The following Anti-Money Laundering/Combating Terrorist Financing (AML/CTF) guidelines are given in support of the Caribbean AML/CTF Principles, which CAIB member banks agreed on as important global guidelines for sound business conduct to ensure the integrity of correspondent banking relationships. The Boards of Directors of CAIB member banks will maintain such policies and procedures that ensure adherence to these Guidelines.

### 1. CLIENT ACCEPTANCE: GENERAL GUIDELINES

#### 1.1 General

Bank policy will be to prevent the use of its operations for criminal purposes. The bank will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate. The primary responsibility for this lies with the senior bank officer who reviews the client for acceptance. Mere fulfillment of internal review procedures does not relieve the bank officer of this basic responsibility. The bank will maintain a Risk Management Committee that will support the operation of these Guidelines.

#### 1.2 Identification

The bank will take reasonable measures to verify the identity of its clients and beneficial owners and will only accept clients when this process has been completed. Clients that are unable to visit the bank in person and have submitted proof of identity documents by mail must have them duly notarized or verified by another established bank or such other specified body

##### 1.2.1 Client

- Natural persons: identity will be established to the bank's satisfaction by reference to official identity papers or such other evidence as may be appropriate under the circumstances.
- Corporations, partnerships, and foundations: the bank will receive documentary evidence of the organization and review its legal existence relative to the laws of the jurisdiction in which the bank operates.
- Trusts: the bank will receive appropriate evidence of formation and existence along with identity of the trustees.
- Identification documents must be current at the time of opening and be scrutinized for good standing.

### 1.2.2 Beneficial owner

Beneficial ownership must be established for all new accounts. Due diligence must be done on all principal beneficial owners identified in accordance with the following principles:

- Natural persons: when the account is in the name of an individual, the bank officer must establish whether the client is acting on his/her own behalf. If doubt exists, the bank will establish the capacity in which and on whose behalf the account holder is acting.
- Legal entities: where the client is a company, such as a private investment company or an international business corporation, the bank officer will understand the structure of the company sufficiently to determine the provider of funds; the principal owner(s) of the shares; and those who have control over the funds, e.g. the directors and those with the power to give direction to the directors of the company. With regard to other shareholders the bank officer will make a reasonable judgment as to the need for further due diligence. This principle applies regardless of whether the share capital is in registered or bearer form. In the latter case, the directors must provide a corporate resolution that confirms the identity of the beneficial owner and supporting material.
- Trusts: where the client is a trustee, the bank officer will understand the structure of the trust sufficiently to determine the provider of funds (e.g. settlor); those who have control over the funds (e.g. trustees); any persons or entities who have the power to remove the trustees; and administrators who have been awarded powers to control the bank account. The bank officer will make a reasonable judgment as to the need for further due diligence.

### 1.2.3 Accounts held in the name of money managers and similar intermediaries

The bank officer will perform due diligence on the intermediary and establish that the intermediary has a due diligence process for its clients, or a regulatory obligation to conduct such due diligence, that is satisfactory to the bank. Such accounts will be identified for ongoing monitoring.

### 1.2.4 Accounts held in the name of banking entities

The bank will not hold accounts for shell banking entities, nor permit the receipt of funds to a client that is for further credit to another beneficiary, unless that client has an approved respondent fiduciary account.

### 1.2.5 Powers of Attorney/Authorized signers

Where the account is to be controlled by a holder of a power of attorney or an authorized signer is appointed by a client, full identification and due diligence on the signatory is required in addition to due diligence on the client. If the client is a legal entity, and the declared beneficial owner is also appointed by the directors as the signatory/POA, it is generally sufficient to do due diligence on the owner/signatory.

### 1.2.6 Practices for electronic banking relations

The bank has determined that relationships initiated through electronic or other communication channels require a higher degree of due diligence prior to account opening. Accounts may not be opened from electronic applications. Any electronic banking services offered are only made available to approved clients that have completed the due diligence process with original documentation either presented in person or submitted by mail.

### 1.3 Due diligence

The bank will collect and record information covering the following categories:

- Purpose and reasons for opening the account
- Government issued identification on all required parties
- Anticipated account activity
- Source of wealth (description of the economic activity which has generated the net worth)
- Estimated net worth
- Source of funds (description of the origin and the means of transfer for monies that are accepted for the account opening)
- References or other sources to corroborate reputation information (e.g. from an established bank and character reference from a professional officer).
- Proof of residence must be confirmed (e.g. from a utility bill, or verified by a bank or other professional officer).

Unless other measures reasonably suffice to conduct the due diligence an application for an account relationship will not be approved.

### 1.4 Oversight responsibility

The bank will require all new clients and new accounts be approved by at least one person other than the bank officer that reviews the application. The bank will ensure that the development and training of key compliance personnel is to the appropriate level of independence and that oversight is established over the compliance department and customer service departments.

### 2. CLIENT ACCEPTANCE: SITUATIONS REQUIRING ADDITIONAL DILIGENCE/ATTENTION

#### 2.1 Numbered or alternate name accounts

Numbered or alternate name accounts will only be accepted if the bank has established and maintains records of the identity of the client and the true beneficial owner, and such accounts must be managed with an appropriate level of scrutiny.

#### 2.2 High-risk countries

The bank will apply heightened scrutiny to clients and beneficial owners resident in and funds sourced from countries identified by credible sources as having inadequate anti-money-laundering standards or representing high-risk for crime and corruption. The bank will take particular care when dealing with countries identified by the Financial Action Task Force (FATF) as non-cooperating countries, and countries associated with sponsoring terrorism.

#### 2.3 International Financial Centre Jurisdictions

Risks associated with entities organized in international financial centre jurisdictions will be covered by enhanced due diligence procedures if those jurisdictions present a greater risk for crime, corruption or terrorist financing.

#### 2.4 High-risk activities

Clients and beneficial owners whose source of wealth emanates from activities which may be susceptible to money laundering will be subject to heightened scrutiny and other specific policies established by the bank. Know Your Customer review and Risk Assessment will determine the acceptance of clients deemed as a higher risk.

#### 2.5 Public officials

Clients who have or have had positions of public trust such as government officials, senior executives of government corporations, politicians, important political party officials, etc. and their families and close associates require heightened scrutiny.

### 3. UPDATING CLIENT FILES

The bank is responsible for updating the client files on a defined basis and/or when there are major changes. The bank's Compliance Officer or an independent control person will review relevant portions of client files on a regular basis to ensure consistency and completeness. The frequency of the reviews or spot checks depends on the size, complexity and risk posed by the account relationship.

### 4. PRACTICES WHEN IDENTIFYING UNUSUAL OR SUSPICIOUS ACTIVITIES

#### 4.1 Definition of unusual or suspicious activities

The bank will maintain a written policy on the identification of and follow-up on unusual or suspicious activities. This policy will include a definition of what is considered to be suspicious or unusual and give examples thereof.

Unusual or suspicious activities may include:

- Account transactions or other activities which are not consistent with the due diligence file
- Transactions over a certain amount
- Pass-through / in-and-out-transactions

#### 4.2 Identification of unusual or suspicious activities

Unusual or suspicious activities can be identified through:

- Monitoring of transactions
- Client contacts (meetings, discussions, in-country visits etc.)
- Third party information (e.g. newspapers, Reuters, Lexis, Internet, foreign court orders, receiverships)
- Bank's knowledge of the client's environment (e.g. political situation in his/her country).

#### 4.3 Follow-up on unusual or suspicious activities

The bank officer, management and/or the compliance officer will carry out an analysis of the background of any unusual or suspicious activity. If there is no plausible explanation a decision will be made involving the compliance function:

- To continue the business relationship with increased monitoring
- To terminate the business relationship
- To report the business relationship to the relevant authorities.

The Compliance Officer designated by senior management will make the suspicious activity report to the authorities. As required by local laws and regulations, the assets may be blocked and transactions may be subject to approval by the Supervisory Authority.

### 5. MONITORING

The bank will require that an appropriate monitoring program be in place. The primary responsibility for monitoring account activities lies with the Compliance Officer and the account relationship officer. Account relationship officers must be familiar with significant transactions and increased activity in the account and will be especially aware of unusual or suspicious activities (see 4.1). The bank will decide to what extent fulfillment of these responsibilities will need to be supported through the use of automated systems or other means, and commit the necessary resources to ensure that on-going monitoring is performed.

### 6. CONTROL RESPONSIBILITIES

The bank will have written procedures in place establishing standard controls to be adopted by the various job functions (account relationship officer, Compliance, Internal Audit).

### 7. REPORTING

The bank will ensure that there is regular management reporting on AML/CTF issues to its Board and Audit Committee (e.g. number of reports to Authorities, monitoring tools, changes in applicable laws and regulations, the number and scope of training sessions provided to employees).

### 8. EDUCATION, TRAINING AND INFORMATION

The bank will conduct a training program on the identification and prevention of money laundering and terrorist financing for employees who have client contact and for Account Relationship and Compliance personnel. Regular training (e.g. annually) will also include how to identify and follow-up on unusual or suspicious activities. In addition, employees will be informed about any major changes in AML/CTF laws and regulations.

All new employees will be informed of these AML/CTF Guidelines.

### 9. RECORD RETENTION REQUIREMENTS

The bank will establish record retention requirements for all AML/CTF related account documents and materials. The documents must be kept for the minimum number of years in accordance with local regulations.

### 10. AML/CTF ORGANIZATION

The bank will provide adequate human resources to be responsible for the prevention of money laundering and combating terrorist financing (e.g. Compliance personnel, Inspections, and Legal).

### 11. COMPLIANCE CULTURE

These Guidelines are sanctioned by the bank's Board of Directors, who provide a top-down approach to encourage the growth of a strong AML/CTF compliance culture throughout the institution

### 12. EXCEPTIONS AND DEVIATIONS

The bank may establish an exception and deviation procedure based on its risk assessment. Approval would need to be sought from the Executive Directors or as determined in the sole discretion of the Board.

Release Version: October 2009